Email Firewall
User Guide

User Guide for the 3Com® Email Firewall

http://www.3com.com/

Part No. DUA-MFA100-AAA01

Published January 2005

POWERED BY BorderWare™

3Com Corporation
350 Campus Drive
Marlborough,
MA 01752-3064

Copyright © 2000-2005, BorderWare Technologies Inc. Used under license by 3Com Corporation. All rights reserved. No part of this documentation may be reproduced in any form or by any means or used to make any derivative work (such as translation, transformation, or adaptation) without written permission from BorderWare Technologies Inc.

3Com Corporation and its licensors reserve the right to revise this documentation and to make changes in content from time to time without obligation on the part of 3Com Corporation or its licensors to provide notification of such revision or change.

3Com Corporation and its licensors provide this documentation without warranty, term, or condition of any kind, either implied or expressed, including, but not limited to, the implied warranties, terms or conditions of merchantability, satisfactory quality, and fitness for a particular purpose. 3Com Corporation and its licensors may make improvements or changes in the product(s) and/or the program(s) described in this documentation at any time.

If there is any software on removable media described in this documentation, it is furnished under a license agreement included with the product as a separate document, in the hard copy documentation, or on the removable media in a directory file named LICENSE.TXT or !LICENSE.TXT. If you are unable to locate a copy, please contact 3Com and a copy will be provided to you.

UNITED STATES GOVERNMENT LEGEND

If you are a United States government agency, then this documentation and the software described herein are provided to you subject to the following:

All technical data and computer software are commercial in nature and developed solely at private expense. Software is delivered as "Commercial Computer Software" as defined in DFARS 252.227-7014 (June 1995) or as a "commercial item" as defined in FAR 2.101(a) and as such is provided with only such rights as are provided in 3Com's standard commercial license for the Software. Technical data is provided with limited rights only as provided in DFAR 252.227-7015 (Nov 1995) or FAR 52.227-14 (June 1987), whichever is applicable. You agree not to remove or deface any portion of any legend provided on any licensed program or documentation contained in, or delivered to you in conjunction with, this User Guide.

Unless otherwise indicated, 3Com registered trademarks are registered in the United States and may or may not be registered in other countries.

3Com, the 3Com logo are registered trademarks of 3Com Corporation.

BorderWare, the Powered by BorderWare Logo, and BorderWare Security Network are trademarks or registered trademarks of BorderWare Technologies Inc. in the United States and other jurisdictions.

Microsoft and Windows are registered trademarks of Microsoft Corporation.

All other company and product names may be trademarks of the respective companies with which they are associated.

ENVIRONMENTAL STATEMENT

It is the policy of 3Com Corporation to be environmentally-friendly in all operations. To uphold our policy, we are committed to:

Establishing environmental performance standards that comply with national legislation and regulations. Conserving energy, materials and natural resources in all operations.

Reducing the waste generated by all operations. Ensuring that all waste conforms to recognized environmental standards. Maximizing the recyclable and reusable content of all products.

Ensuring that all products can be recycled, reused and disposed of safely.
Ensuring that all products are labelled according to recognized environmental standards.

Improving our environmental record on a continual basis.

End of Life Statement

3Com processes allow for the recovery, reclamation and safe disposal of all end-of-life electronic components.

Regulated Materials Statement

3Com products do not contain any hazardous or ozone-depleting material.

Environmental Statement about the Documentation

The documentation for this product is printed on paper that comes from sustainable, managed forests; it is fully biodegradable and recyclable, and is completely chlorine-free. The varnish is environmentally-friendly, and the inks are vegetable-based with a low heavy-metal content.

ENCRYPTION

This product contains encryption and may require U.S. and/or local government authorization prior to export or import to another country.

CONTENTS

ABOUT THIS GUIDE

Conventions 10
Related Documentation 11
Documentation Comments 11

1 3COM EMAIL FIREWALL OVERVIEW

Deployment and Installation 13
  Installation 14
Features 14
  Anti-Spam 14
  Anti-Virus Scanning 14
  Malformed Email Checks 14
  Attachment Control 15
  Email Security 15
  Reporting 15
System Administration 16
  Main Menu 17

2 CONFIGURING MAIL DELIVERY

Mail Routing 19
  Additional Mail Route Rules 21
Delivery Settings 23
  Delivery Settings 23
  Gateway Features 23
  Default Mail Relay 23
  BCC All Mail 24
  Annotations 24
  Advanced Delivery Settings 25
Mail Mappings 26
  Uploading Mapping List 27

Virtual Mappings 28
Uploading Virtual Mapping List 29

3 CONFIGURING MAIL SECURITY
Anti-Virus 31
Notifications 33
Pattern Files 33
Attachment Control 34
Notifications 35
Editing Attachment Types 36
Mail Access/Filtering 37
Specific Access Patterns 38
Pattern Based Message Filtering 39
Message Restrictions 39
SMTP Authenticated Relay 40
SMTP Banner 40
SMTP Security 41
Incoming Mail 42
Mail Delivery 42
Malformed Email 44

4 ANTI-SPAM CONFIGURATION
Anti-Spam Features 47
DCC 49
STA 50
Spam Action 52
Maybe Spam Action 52
Diagnostics 53
STA Training 54
Pattern Based Message Filtering 54
Message Part 55
Match Option 58
Pattern 58
Priority 58
Action 58
Upload or Download File 59
PBMF Preferences 59

59
Objectionable Content Filtering 61
Actions 61
Notifications 62
Upload and Download Filter List 62
Trusted Senders List 62
Adding Trusted Senders 63
Spam Quarantine 64
Spam Quarantine Configuration 64
User Notification 65
Set Redirect Action for Anti-Spam Features 65
Enabling User Access on a Network Interface 66
Examining the Quarantine 66
Quarantine and Trusted Senders List Users 67
Upload and Download User Lists 68
Enabling User Access on a Network Interface 68
Advanced Anti-Spam Options 69
RBL (Realtime Blackhole List) 69
Mail Access/Filtering 70
Anti-Spam Header 70

5 REPORTING
Generating Reports 71
Report Configuration 72
Report Generation 73
Report Fields 74
System Logs 77
Viewing Log Details 78
Configuring a Syslog Server 78
Email History 79
System History 80
Event Types 80
Configure History Settings 82

6 SYSTEM CONFIGURATION
Setup Wizard 83
Change Password 84

Time Zone 84
Network Configuration 85
Mail Configuration 85
Admin Account 86
System Users 86
Creating an Admin User 87
Upload and Download User Lists 88
Enabling User Access on a Network Interface 88
Network Settings 89
Network Interfaces 90
Advanced Parameters 90
Web Proxy 91
Static Routes 92
Licensing 93
Installed License 93
License Agreements 94
License Renewal or Upgrade 94
SSL Certificates 94
Software Updates 96
Uploading a Software Update 96
Security Connection 97

7 SYSTEM MANAGEMENT

Status and Utility 99
Utility Functions 100
Current Admin and Spam Quarantine Users 104
Configuration Information 104
Mail Queues 104
Quarantine 105
Expiry Settings 105
Daily Tasks 106
Backup and Restore 107
Starting a Backup 107
Restores 111
Reboot and Shutdown 113
Reset to Factory Settings 113

8 MONITORING ACTIVITY AND STATUS
Monitoring Mail Processing Activity 115
Mail Server Status 116
Mail Queue (Mail Q) 116
Mail Queue Statistics 116
Mail Received Recently 116
Troubleshooting Mail Queue Problems 116
Email Firewall Status 117
System Alarms 118
Licensing 118
BorderWare Mail Security Services 118
Network Settings 118
Report Problems 119
Troubleshooting Mail Delivery Problems 120
Examining Log Files 121
Troubleshooting Content Issues 123
Email History 123

A CUSTOMIZING SYSTEM MESSAGES

B RESET TO FACTORY DEFAULT SETTINGS FROM CONSOLE

C THIRD PARTY COPYRIGHT AND LICENSE AGREEMENTS

GLOSSARY

About This Guide

The instructions in this guide are designed to help you with configuration and system administration tasks for the 3Com® Email Firewall.

This guide is intended for the system or network administrator who is responsible for configuring, using, and managing the 3Com Email Firewall. It assumes a working knowledge of TCP/IP network and email communications protocols.

For more detailed information on 3Com Email Firewall installation, please see the accompanying Installation Guide.

If release notes are shipped with your product and the information there differs from the information in this guide, follow the instructions in the release notes.

Most user guides and release notes are available in Adobe Acrobat Reader Portable Document Format (PDF) or HTML on the 3Com World Wide Web site:

http://www.3com.com/products

Conventions

Table 1 and Table 2 list conventions that are used throughout this guide.

Table 1 Notice Icons

Icon	Notice Type	Description
	Information note	Information that describes important features or instructions
	Caution	Information that alerts you to potential loss of data or potential damage to an application, system, or device
	Warning	Information that alerts you to potential personal injury

Table 2 Text Conventions

Convention	Description
`Screen displays`	This typeface represents information as it appears on the screen.
`Syntax`	The word "syntax" means that you must evaluate the syntax provided and then supply the appropriate values for the placeholders that appear in angle brackets. Example: To change your password, use the following syntax: `system password <password>` In this example, you must supply a password for <password>.
`Commands`	The word "command" means that you must enter the command exactly as shown and then press Return or Enter. Commands appear in bold.
The words "enter" and "type"	When you see the word "enter" in this guide, you must type something, and then press Return or Enter. Do not press Return or Enter when an instruction simply says "type."
Keyboard key names	If you must press two or more keys simultaneously, the key names are linked with a plus sign (+). Example: Press Ctrl+Alt+Del
Words in *italics*	Italics are used to: ■ Emphasize a point. ■ Denote a new term at the place where it is defined in the text. ■ Identify menu names, menu commands, and software button names. Examples: From the *Help* menu, select *Contents*. Click *OK*.

Related Documentation

In addition to this guide, each 3Com Email Firewall documentation set includes the following:

- *3Com Email Firewall Installation Guide*

  This guide contains detailed information on installing the 3Com Email Firewall.

- *Release Notes*

  These notes provide information about the current software release, including new features, modifications, and known problems.

Documentation Comments

Your suggestions are very important to us. They will help make our documentation more useful to you. Please send comments about this document to 3Com via the following URL:

http://www.3com.com/corpinfo/en_US/contactus/index.html

Please include the following information when contacting us:

- Document title
- Document part number (on the title page)
- Page number (if appropriate)

Example:

- 3Com Email Firewall User Guide
- Part number: DUA-MFA100-AAA01
- Page 25

Please note that we can only respond to comments and questions about 3Com product documentation. Questions related to technical support or sales should be directed in the first instance to your network supplier.

1 3COM EMAIL FIREWALL OVERVIEW

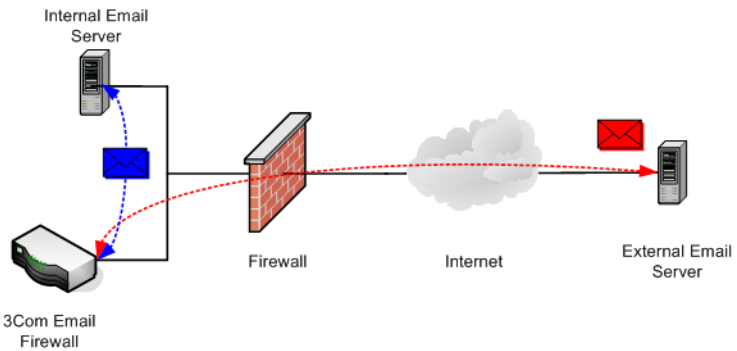
This chapter provides an overview of the 3Com Email Firewall and its features, and includes the following topics:

- Deployment and Installation
- Features
- System Administration

Deployment and Installation

The 3Com Email Firewall is designed to be situated between your mail servers and the Internet so that there are no direct SMTP (Simple Mail Transport Protocol) connections between external and internal servers.

The 3Com Email Firewall is installed behind the existing firewall on the Internal network.



Inbound mail will be forwarded from the Firewall or Router to the 3Com Email Firewall where it will be scanned, processed, and then sent to your internal mail server for delivery.

Outbound mail will be sent from your internal mail server to the 3Com Email Firewall to be scanned, processed, and then delivered to the destination SMTP server on the Internet.

Installation

For detailed information on installation, see the *Installation Guide* that came with your 3Com Email Firewall.

Features

The following sections provide an overview of the main features of the 3Com Email Firewall.

Anti-Spam

The 3Com Email Firewall contains a variety of powerful features to prevent spam messages, including the following:

- Server-based tools such as DCC (Distributed Checksum Clearinghouse), STA (Statistical Token Analysis), Objectionable Content Filtering, and Pattern Based Message Filtering that prevent spam messages from being delivered to an end user's mailbox.
- User-based tools for managing quarantined spam and building trusted senders lists for whitelisting.

Anti-Virus Scanning

The 3Com Email Firewall provides a built-in virus scanning service. When enabled, all messages (inbound and outbound) passing through the 3Com Email Firewall are scanned for viruses.

Viruses can be selectively blocked depending on whether they are found in inbound or outbound messages. Message attachments are recursively disassembled to help ensure that viruses cannot be concealed.

Malformed Email Checks

Many viruses try to elude virus scanners by concealing themselves in malformed messages. The scan engines cannot detect the attachment and pass the complete message through to an internal server.

Some mail clients try to rebuild malformed messages and may rebuild or activate a virus-infected attachment. Other types of malformed messages are designed to attack mail servers directly. These types of messages are often used in denial-of-service (DoS) attacks.

The 3Com Email Firewall analyzes each message with very extensive integrity checks. Malformed messages are quarantined if they cannot be processed.

Attachment Control

Attachment filtering can be used to control a wide range of problems originating from the use of attachments, such as viruses, objectionable content, and confidential documents leaving your network.

Both inbound and outbound email can be scanned. Messages containing forbidden attachments can be rejected or quarantined.

Email Security

Communications between email gateways that are normally sent in clear text can be protected from interception and eavesdropping via TLS (Transport Layer Security) encryption.

Reporting

The 3Com Email Firewall's reporting features allow you to create customized reports on mail and system activity, including the following:

- Traffic Summary
- System Health
- Top Mailbox Disk Users
- Spam Statistics
- Virus Reports
- Email History
- System Events History

The reports are derived from information written to the various systems logs and then stored in the database. Reports are stored on the system for online viewing and can also be emailed automatically to specified users.

System Administration

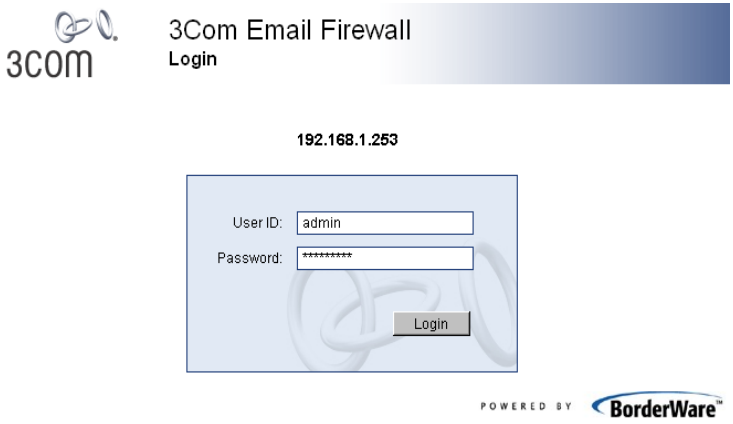
The 3Com Email Firewall is administered via a web browser. The following web browsers are supported:

- Microsoft Internet Explorer 5.5 or greater
- Netscape 7.0 or greater
- Mozilla Firefox 1.0 or greater
- Safari 1.2.3 or greater

Your web browser must have cookies enabled to be able to connect and login to the 3Com Email Firewall.

Launch a web browser on your computer and enter the IP address or hostname into the location bar, such as **https://192.168.1.253**, or **https://mail.example.com**.

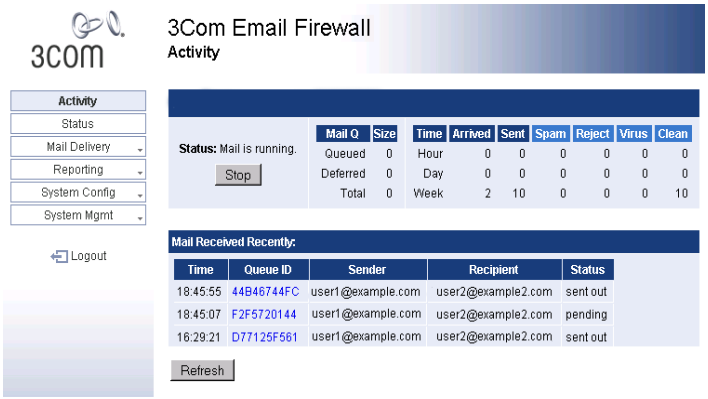
The login screen will then be displayed. Enter the user name **admin** and the corresponding password.



The *Activity* screen and main menu will then be displayed.

Main Menu

The main menu provides quick access to the 3Com Email Firewall's configuration and management options.



The menu is divided into the following sections:

- Activity — The *Activity* screen provides you with a variety of information on mail processing activity, such as the number of messages in the mail queue, the number of different types of messages received and sent, and current message activity.
- Status — The *Status* page displays a list of system services and their current status. Network and system tests can also be performed.
- Mail Delivery — This menu allows you to configure mail delivery features such as:
  - Anti-Spam
  - Anti-Virus
  - Attachment Control
  - Mail Routing
  - Delivery Settings
  - Mail Access/Filtering
  - Mail Mappings
  - Virtual Mappings
  - SMTP Security
  - Malformed Email detection

- Reporting — This menu allows you to view and configure the reporting and system log features of the 3Com Email Firewall.
- System Configuration — This menu allows you to view and modify system configuration settings such as:
  - The Setup Wizard
  - Admin Account
  - System Users
  - Network Settings
  - Web Proxy
  - Static Routes
  - Licensing
  - SSL Certificates
  - Software Updates
- System Management — This menu is used for system management features such as:
  - Status and Utility menu for troubleshooting
  - Mail Queues
  - Quarantine
  - Backup and Restore
  - Reboot and Shutdown
  - Returning the system to factory settings

2 CONFIGURING MAIL DELIVERY

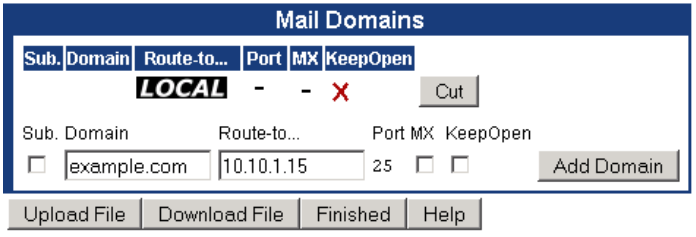
This chapter describes how to configure your 3Com Email Firewall to accept and deliver mail, and includes the following topics:

- Mail Routing
- Delivery Settings
- Mail Mappings
- Virtual Mappings

Mail Routing

Mail Routes are used to define the domains you will be accepting mail for, and where locally to deliver the mail such as an internal Microsoft® Exchange mail server. The Mail Domain you configured at installation time using the Setup Wizard will automatically be created.

Select **Mail Delivery -> Mail Routing** from the menu to define additional mail routes.



- Sub — Select this check box to accept and relay subdomains for the specified domain.
- Domain — Enter the domain for which mail is to be accepted, such as *example.com*.

- Route-to — Enter the address for the mail server to which mail will be delivered. This is your local mail server, such as a Microsoft Exchange mail system.
- MX — (Optional) Select the MX check box if you need to look up the mail routes in DNS before delivery. If this is not enabled, MX records will be ignored. Generally, you do not need to select this item unless you are using multiple mail server DNS entries for load balancing/failover purposes. By checking the MX record, DNS will be able to send the request to the next mail server in the list.
- KeepOpen — (Optional) Select the KeepOpen check box to ensure that each mail message to the domain will not be removed from the active queue until delivery is attempted, even if the preceding mail failed or was deferred. This setting ensures that local mail servers receive high priority.

The KeepOpen option should only be used for domains that are usually very reliable. If the domain is unavailable, it may cause system performance problems due to excessive error conditions and deferred mail.

A list of domains can also be uploaded in one text file. The file must contain comma or tab separated entries in the form:

[domain],[route],[port],[ignore_mx],[subdomains_too],[keep_open]

For example:

example.com,10.10.1.1,25,on,off,off

The file (*domains.csv*) should be created in csv file format using Excel, Notepad or other Windows text editor. It is recommended that you download the domain file first by clicking **Download File**, editing it as required, and uploading it using the **Upload File** button.

Additional Mail Route Rules

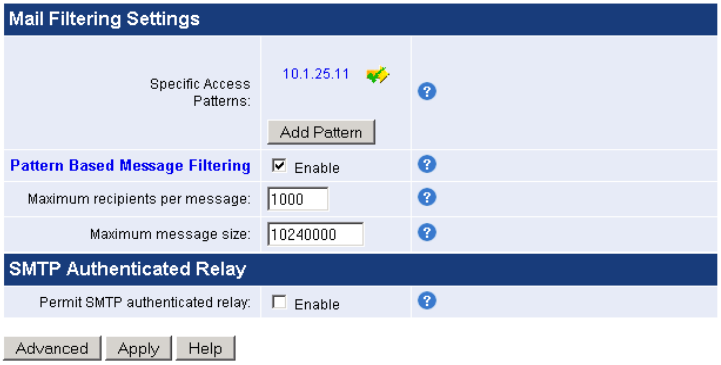
When adding an additional mail route for a local email server, you must add a **Specific Access Pattern** and a **Pattern Based Message Filter** to trust mail from that server for Anti-Spam training purposes.

These procedures are not required for the default mail route you configured at installation time with the Setup Wizard.

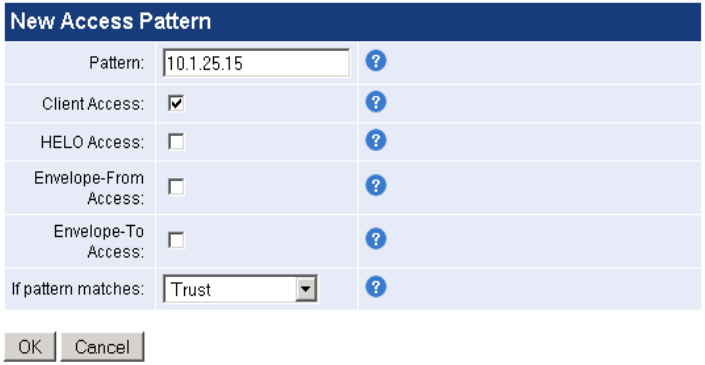
Adding a Specific Access Pattern

1 Select **Mail Delivery -> Mail Access/Filtering** from the menu.

Your primary mail route defined during installation will already be configured.



2 Click **Add Pattern** to add a new pattern for the additional mail route.



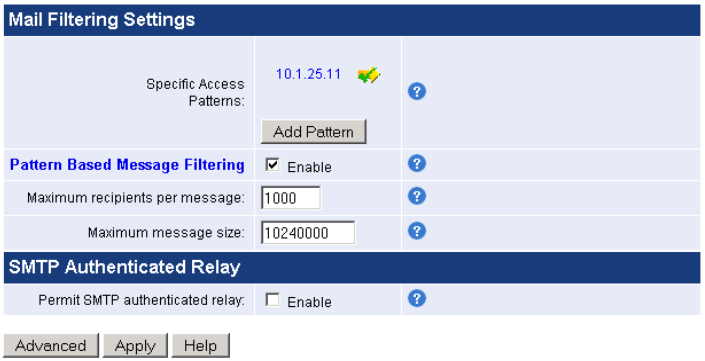
3 Enter the IP address of the mail server you are routing to in the *Pattern* field.

4 Select *Client Access*

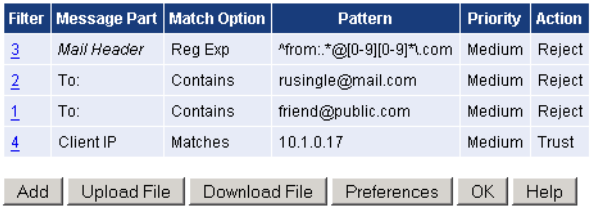
5 Select **Trust** for the action if the pattern matches, and click **OK**.

Adding a Pattern Based Message Filter

1 Select **Mail Delivery -> Mail Access/Filtering** from the menu. Select **Pattern Based Message Filtering**.



2 Click **Add** to add a new filter rule.



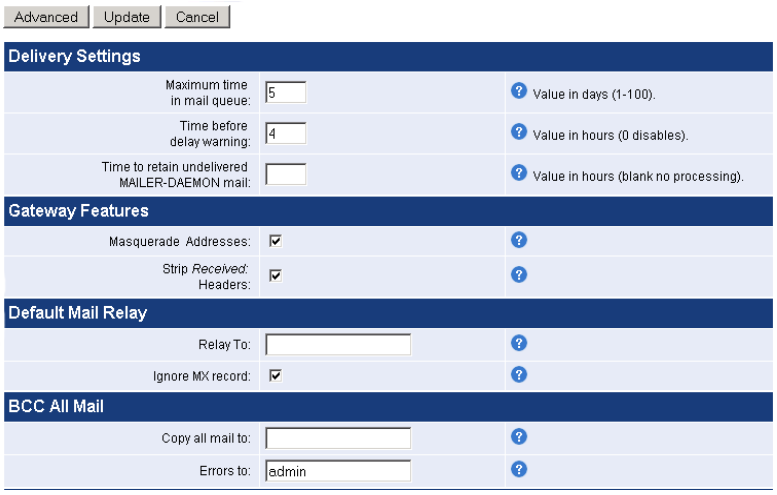
3 Select **Client IP** as the *Message Part*, and set the address of the mail server for the mail route as the pattern.

4 Set the *Action* to **Trust** and click **Update** to add the new rule.

Delivery Settings

You can customize various delivery settings that affect how you accept and deliver mail messages.

Select **Mail Delivery -> Delivery Settings** from the menu.



Delivery Settings

- Maximum time in mail queue — Enter the number of days for a message to stay in the queue before being returned to the sender as "undeliverable."
- Time before delay warning — Number of hours before issuing the sender a notification that mail is delayed.
- Time to retain undelivered MAILER-DAEMON mail — The number of hours to keep undelivered mail addressed to MAILER-DAEMON (the internal mail server process.)

Gateway Features

- Masquerade Addresses — Masquerades internal hostnames by rewriting headers to only include the address of the 3Com Email Firewall.
- Strip Received Headers — Strip all Received headers from outgoing messages.

Default Mail Relay

- Relay To — (Optional) Enter an optional hostname or IP address of a mail server (not this 3Com Email Firewall) to relay mail to for all email with unspecified destinations. A recipient's email domain will be

checked against the Mail Routing table, and if the destination is not specified the email will be sent to the Default Mail Relay server for delivery. This option is typically used when the 3Com Email Firewall cannot deliver email directly to remote mail servers.

- Ignore MX record — Enable this option to prevent an MX record lookup for this host to force relay settings.

BCC All Mail

The 3Com Email Firewall offers an archiving feature for organizations that require storage of all email that passes through their corporate mail servers. This option sends a blind carbon copy (BCC) of each message that passes through the 3Com Email Firewall to the specified address. This address can be local or on any other system. Once copied, the mail can be effectively managed and archived from this account.

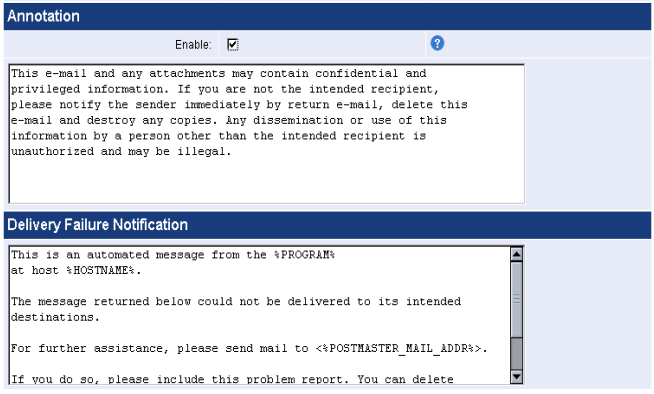
- Copy all mail to — Enter an email address to copy mail to.
- Errors to — Specify an address that will receive error messages if there are problems delivering the BCC mail.

Annotations

In the *Annotations* section, you can enable annotations that are appended to all emails and customize *Delivery Failure* and *Delivery Delay Warning* messages.

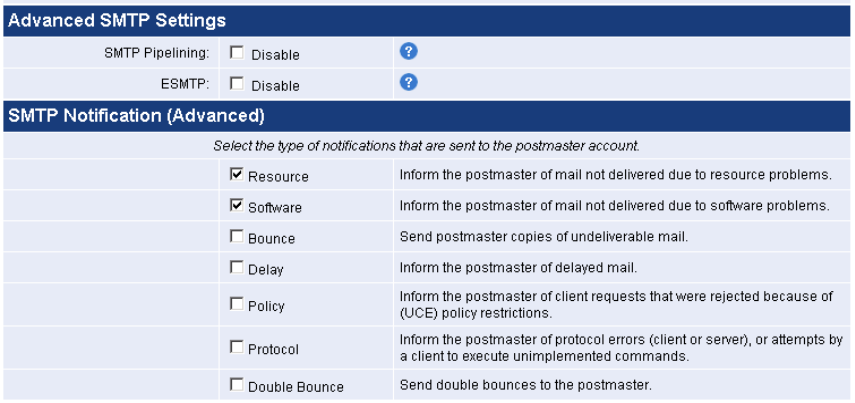
The variables in the messages, such as *%PROGRAM%* and *%HOSTNAME%*, are local system settings that are automatically substituted at the time the message is sent.

See Appendix A "Customizing System Messages" on page 125 for a full list of variables that can be used.


Annotation
Enable:
This e-mail and any attachments may contain confidential and privileged information. If you are not the intended recipient, please notify the sender immediately by return e-mail, delete this e-mail and destroy any copies. Any dissemination or use of this information by a person other than the intended recipient is unauthorized and may be illegal.
Delivery Failure Notification
This is an automated message from the %PROGRAM% at host %HOSTNAME%.
The message returned below could not be delivered to its intended destinations.
For further assistance, please send mail to <%POSTMASTER_MAIL_ADDR%>.
If you do so, please include this problem report. You can delete

Advanced Delivery Settings

Click the **Advanced** button to reveal options for advanced SMTP (Simple Mail Transport Protocol) settings and SMTP notifications.


Advanced SMTP Settings
SMTP Pipelining:
Disable
ESMTP:
Disable
SMTP Notification (Advanced)
Select the type of notifications that are sent to the postmaster account.
Resource
Inform the postmaster of mail not delivered due to resource problems.
Software
Inform the postmaster of mail not delivered due to software problems.
Bounce
Send postmaster copies of undeliverable mail.
Delay
Inform the postmaster of delayed mail.
Policy
Inform the postmaster of client requests that were rejected because of (UCE) policy restrictions.
Protocol
Inform the postmaster of protocol errors (client or server), or attempts by a client to execute unimplemented commands.
Double Bounce
Send double bounces to the postmaster.

Advanced SMTP Settings

- SMTP Pipelining — Pipelining allows more than one SMTP command to be inserted into a network packet which reduces SMTP connection times. Some mail servers may experience problems with SMTP command pipelining and you may have to disable this feature if required.
- ESMTP — ESMTP (Extended SMTP) extends basic SMTP functionality to support additional media types in email messages. Some mail servers may not support ESMTP and you may have to disable this feature if you are experiencing problems.

SMTP Notification (Advanced)

Select the type of notifications that are sent to the postmaster account.

- Resource — Mail not delivered due to resource problems such as queue file write errors.
- Software — Mail not delivered due to software problems.
- Bounce — Send postmaster copies of undeliverable mail. If mail is undeliverable, a single bounce message is sent to the postmaster with a copy of the message that was not delivered. For privacy reasons, the postmaster copy is truncated after the original message headers. If a single bounce message is undeliverable, the postmaster receives a

double bounce message with a copy of the entire single bounce message.

- Delay — Inform the postmaster of delayed mail. In this case, the postmaster receives message headers only.
- Policy — Inform the postmaster of client requests that were rejected because of unsolicited mail policy restrictions. The postmaster will receive a transcript of the entire SMTP session.
- Protocol — Inform the postmaster of protocol errors (client or server), or attempts by a client to execute unimplemented commands. The postmaster will receive a transcript of the entire SMTP session.
- Double Bounce — Send double bounces to the postmaster.

Mail Mappings

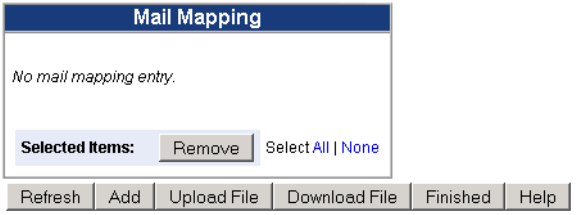
Mail Mappings are used to map an external address to a different internal address and vice versa. This is useful for hiding internal mail server addresses from external users.

For mail originating externally, the mail mapping translates the address in the To: and CC: mail header field into a corresponding internal address to be delivered to a specific internal mailbox.

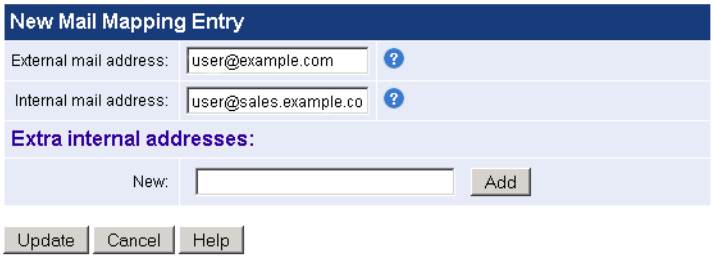
For example, mail addressed to *user@example.com* can be redirected to the internal mail address *user@sales.example.com*. This enables the message to be delivered to the user's preferred mailbox.

Similarly, mail originating internally will have the address in the From:, Reply-To:, and Sender: header modified by a mail mapping so it appears to have come from the preferred external form of the mail address, *user@example.com*.

Select **Mail Delivery -> Mail Mappings** to configure your mail mappings.



Click **Add** to add a new mapping to your list.



- External mail address — Enter the external mail address that you want to be converted to the specified internal email address for incoming mail. The specified internal address will be converted to this external address for outgoing mail.
- Internal mail address — Enter the internal mail address that you want external addresses to be mapped to for incoming mail. The internal address will be converted to the specified external address for outgoing mail.
- Extra internal addresses — Enter any additional internal mappings that will be included in the outgoing mail conversion.

Click **Update** when finished.

Uploading Mapping List

A list of mappings can also be uploaded in one text file. The file must contain comma or tab separated entries in the form:

["sender" or "recipient"],[map_in],[map_out],[value ("on" or "off")]

For example:

sender,user@example.com,user@sales.example.com,on

The file (*mailmapping.csv*) should be created in csv file format using Excel, Notepad or other Windows text editor. It is recommended that you download the mail mapping file first by clicking **Download File**, editing it as required, and uploading it using the **Upload File** button.

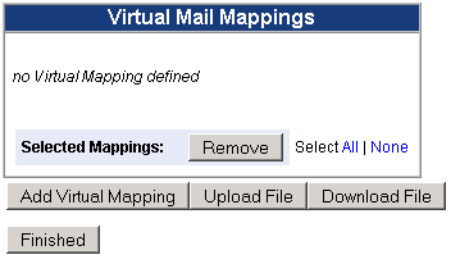
Virtual Mappings

Virtual Mappings are used to redirect mail addressed for one domain to a different domain. This process is performed without modifying the To: and From: headers in the mail, as virtual mappings modify the envelope-recipient address.

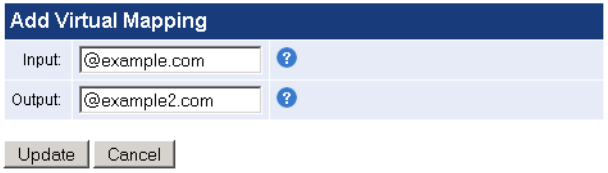
For example, the 3Com Email Firewall can be configured to accept mail for *example.com* and deliver it to *example2.com*. This allows the 3Com Email Firewall to distribute mail to multiple internal servers based on the Recipient: address of the incoming mail.

Virtual Mappings are useful for acting as a wildcard mail mapping, such as mail for *example.com* is sent to *exchange.example.com*.

Select **Mail Delivery -> Virtual Mappings** to configure your mappings.



Click the **Add Virtual Mapping** button to add a new mapping.



- Input — Enter the domain or address to which incoming mail is directed in the Input box.
- Output — Enter the domain or address to which mail should be redirected to in the Output box.

Uploading Virtual Mapping List

A list of virtual mappings can also be uploaded in one text file. The file must contain comma or tab separated entries in the form:

```
[map_in],[map_out]
```

For example:

```
user@example.com,user
user@example.com,user@example2.com
@example.com,@example2.com
```

The file (*virtmap.csv*) should be created in csv file format using Excel, Notepad or other Windows text editor. It is recommended that you download the virtual mapping file first by clicking **Download File**, editing it as required, and uploading it using the **Upload File** button.

3 CONFIGURING MAIL SECURITY

This chapter describes how to configure mail security settings on your 3Com Email Firewall, and includes the following topics:

- Anti-Virus
- Attachment Control
- Mail Access/Filtering
- SMTP Security
- Malformed Email

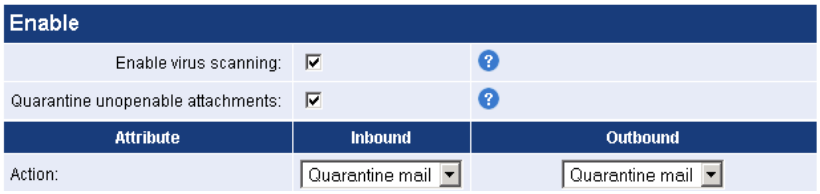
Anti-Virus

The 3Com Email Firewall provides a built-in virus scanning service. When enabled, all messages (inbound and outbound) passing through the 3Com Email Firewall are scanned for viruses.

Viruses can be selectively blocked depending on whether they are found in inbound or outbound messages. Message attachments are recursively disassembled to help ensure that viruses cannot be concealed.

When a virus-infected message is received, it can be deleted, quarantined, or the event can be logged. Quarantined messages may be viewed, forwarded, downloaded, or deleted. Quarantined messages can also be automatically deleted based on their age.

Select **Mail Delivery -> Anti-Virus** from the menu to enable and configure virus scanning.



- Enable virus scanning — Select the check box to enable virus scanning.
- Quarantine unopenable attachments —This option is enabled by default to quarantine attachments that are password-protected and flag them in the logs as "suspicious". This feature prevents password-protected zip files that contain viruses or worms from being passed through the system.

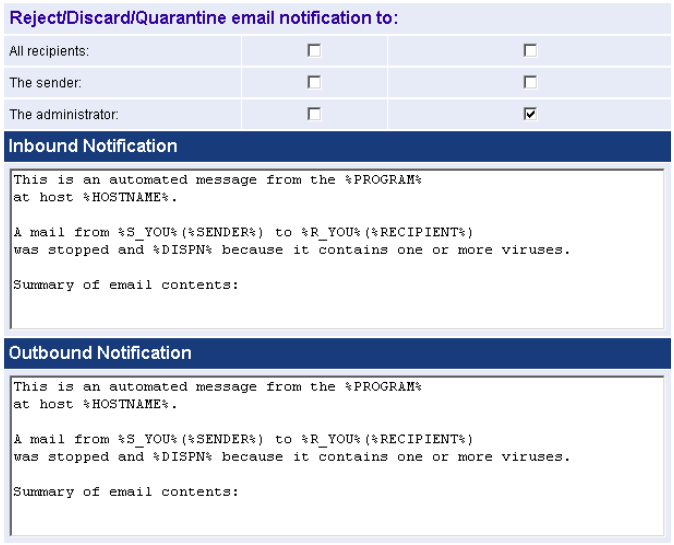
This option will only take effect if the Anti-Virus action is set to Quarantine Mail.

- Action — Configure the action for both inbound and outbound mail. Possible actions include:
  - Just log: Log the event and take no further action.
  - Reject mail: The message is rejected with notification to the sending system.
  - Quarantine mail: The message is placed into quarantine.
  - Discard mail: The message is discarded without notification to the sending system.

*You can view and manage the quarantine area by selecting **System Mgmt -> Quarantine** from the menu. See "Quarantine" on page 105 for more information on the Quarantine area.*

Notifications

Notifications for inbound and outbound messages can be enabled for all recipients, the sender, and the administrator. Customize the content for the *Inbound* and *Outbound* notification in the corresponding text boxes.

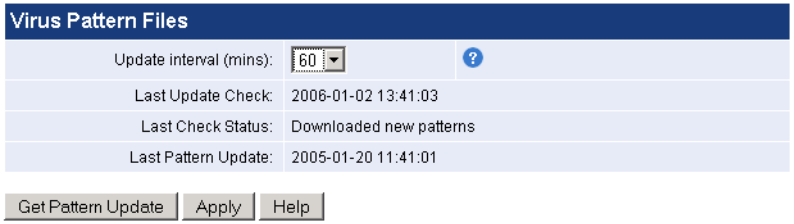

Reject/Discard/Quarantine email notification to:
All recipients:
The sender:
The administrator:
Inbound Notification
This is an automated message from the %PROGRAM%
at host %HOSTNAME%.
A mail from %S_YOU%(%SENDER%) to %R_YOU%(%RECIPIENT%)
was stopped and %DISPN% because it contains one or more viruses.
Summary of email contents:
Outbound Notification
This is an automated message from the %PROGRAM%
at host %HOSTNAME%.
A mail from %S_YOU%(%SENDER%) to %R_YOU%(%RECIPIENT%)
was stopped and %DISPN% because it contains one or more viruses.
Summary of email contents:

See Appendix A "Customizing System Messages" *on* page 125 *for a full list of variables that can be used.*

Pattern Files

Virus pattern files must be continuously updated to ensure that you are protected from new virus threats. The frequency of virus pattern file updates can be configured in the *Virus Pattern Files* section.

Select the time interval to check for pattern file updates. Options include 15, 30, and 60 minutes.



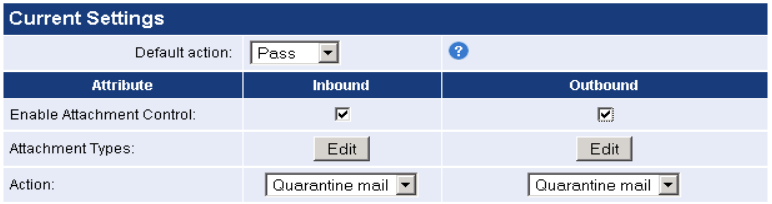
Click the **Get Pattern Update** button to retrieve a new pattern update file immediately.

Attachment Control

Attachment filtering can be used to control a wide range of problems originating from the use of attachments, including the following:

- Viruses — Attachments that can potentially contain viruses can be blocked.
- Offensive Content — The 3Com Email Firewall can block the transfer of images which reduces the possibility that an offensive picture will be transmitted to or from your company mail system.
- Confidentiality — Prevents unauthorized documents from being transmitted through the 3Com Email Firewall.
- Productivity — Prevents your systems from being abused by employees.

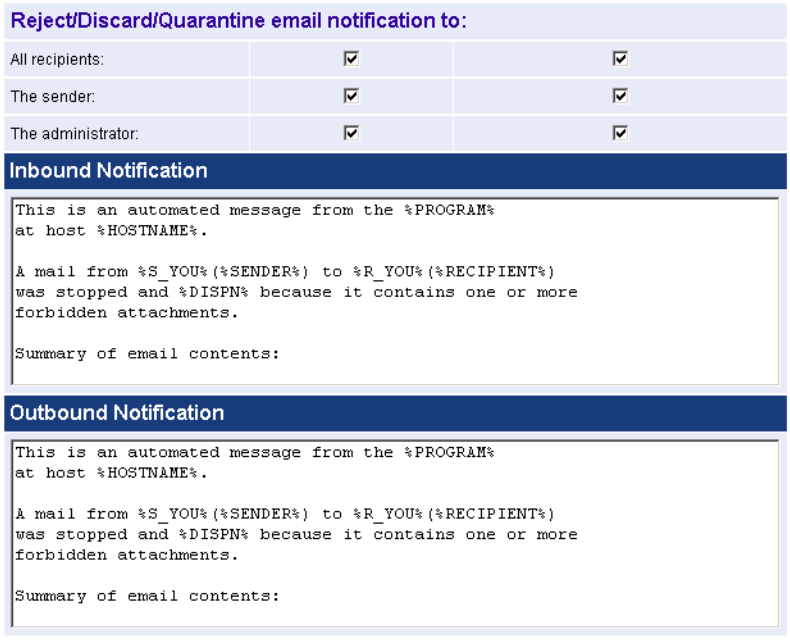
Select **Mail Delivery -> Attachment Control** from the menu to configure your attachment types and actions.



- Default action — Set the default attachment control action for items not specifically listed in the *Attachment Types* list. The default is "Pass" which allows all attachments. Any file types defined in the *Attachment Types* list will override the default setting.
- Enable Attachment Control — Select the check box to enable Attachment Control for inbound and/or outbound mail.
- Attachment Types — Click **Edit** to configure the attachment types.
- Action — Select an action to be performed. Options include:
  - Just log: Log the event and take no further action.
  - Reject mail: The message is rejected with notification to the sending system.
  - Quarantine mail: The message is placed into quarantine.
  - Discard mail: The message is discarded without notification to the sending system.

Notifications

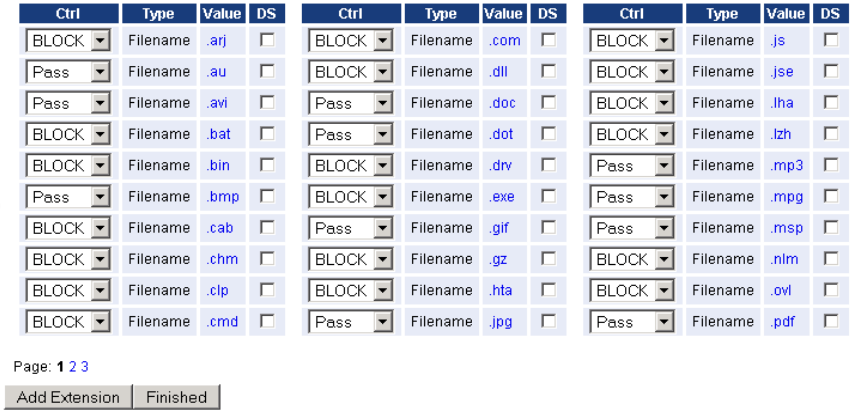
Notifications for inbound and outbound messages can be enabled for all recipients, the sender, and the administrator. Customize the content for the *Inbound* and *Outbound* notification in the corresponding text boxes.


Reject/Discard/Quarantine email notification to:
All recipients:
The sender:
The administrator:
Inbound Notification
This is an automated message from the %PROGRAM%
at host %HOSTNAME%.
A mail from %S_YOU%(%SENDER%) to %R_YOU%(%RECIPIENT%)
was stopped and %DISPN% because it contains one or more
forbidden attachments.
Summary of email contents:
Outbound Notification
This is an automated message from the %PROGRAM%
at host %HOSTNAME%.
A mail from %S_YOU%(%SENDER%) to %R_YOU%(%RECIPIENT%)
was stopped and %DISPN% because it contains one or more
forbidden attachments.
Summary of email contents:

See Appendix A "Customizing System Messages" *on* page 125 *for a full list of variables that can be used.*

Editing Attachment Types

Click the **Edit** button to edit your attachment types. You can add file extensions (*.mp3*), or MIME content types (*image/gif*). For each attachment type, choose whether you want to "BLOCK" or "Pass" the attachment.



Select the *DS (Disable Content Scan)* check box if you want to disable content scanning for attachments with the specified extension. The attachment will still be checked for viruses if the *Disable Content Scan* option is selected.

Click the **Add Extension** button to add a file extension or MIME type to the list, and then click **Update**.

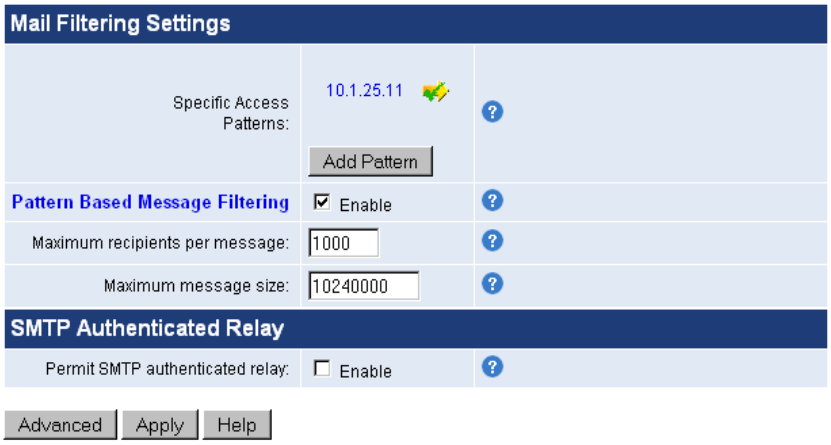
The following example adds a MIME type of *image/png* to the attachment types list.

Mail Access/Filtering

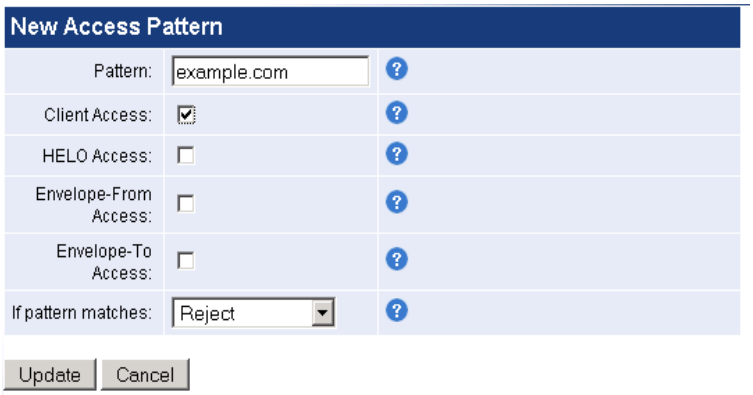
The 3Com Email Firewall provides a number of filtering options to ensure that specific mail messages are not accepted from the incoming SMTP connection.

In the *Mail Access/Mail Filtering* settings, you can specify patterns to match for on incoming connections and configure an appropriate action. The maximum number of recipients and the maximum size of a message can also be configured.

Select **Mail Delivery -> Mail Access/Filtering** to configure access patterns and mail filters.



Specific Access Patterns Click the **Add Pattern** button to add a new specific access pattern.



- Pattern — Enter a mail address, hostname, domain name, or IP Address.
- Client Access — This parameter is used for domain, hostname, or IP address patterns. This item is the most reliable and may be used to block spam as well as whitelist.

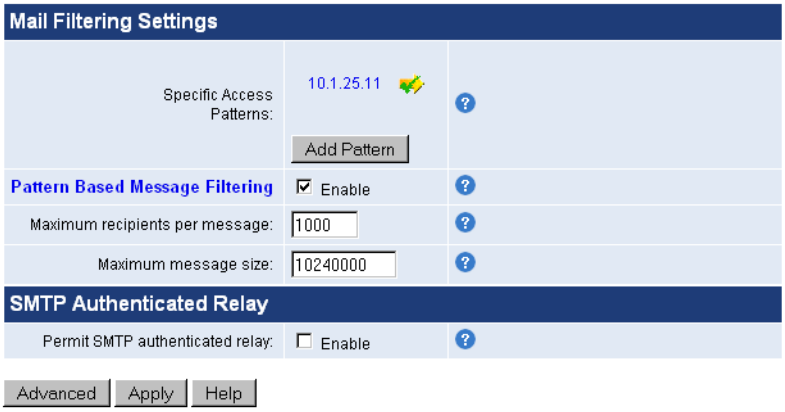
Only the Client Access parameter can be relied upon because spammers can easily forge all other message properties. The other parameters, however, are useful for whitelisting.

- HELO Access — This parameter requires either a domain or hostname pattern. It is not reliable as spammers can fake this property.
- Envelope-From Access — This parameter requires a valid email address pattern. It is not reliable as spammers can fake this property.
- Envelope-To Access — This parameter requires a valid email address pattern. It is not reliable as spammers can fake this property.
- If Pattern Matches:
  - Reject: The connection will be dropped.
  - Allow relaying: Messages from this address will be relayed and processed for spam.
  - Trust: Messages from this address will be relayed and not processed for spam.

Pattern Based Message Filtering

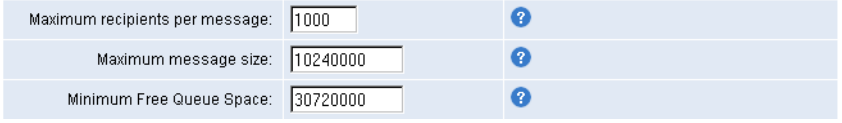
Pattern Based Message Filtering is the primary tool for whitelisting and blacklisting messages. An administrator can specify that mail is rejected or whitelisted according to the contents of the message envelope, message header (such as the sender, recipient, subject), and body text.

See "Pattern Based Message Filtering" on page 54 for more details on configuring these types of filters.



Message Restrictions

The following parameters allow you to reject messages based on the number of recipients, the message size, or free queue space available.



- Maximum recipients per message — Set the maximum number of recipients accepted per message. This helps prevent delivery of spam messages that typically contain a large number of recipients.
- Maximum message size — Set the maximum message size (in bytes) that will be accepted by the 3Com Email Firewall. Ensure that the specified size can accommodate email attachments.
- Minimum Free Queue Space (Advanced)— Set the minimum free queue space available (in bytes) before the system will stop receiving mail. This option only appears if you click the **Advanced** button.

SMTP Authenticated Relay

This feature allows authenticated clients to use the 3Com Email Firewall as an external mail relay for sending mail. For example, you may have remote users that need to send mail via this system.

Client systems must use a login and password to authenticate to the system before being allowed to relay mail. Authenticated relay can also allow authorized mail servers to use this 3Com Email Firewall as a relay. Users must have a local account on this 3Com Email Firewall for the feature to work.

It is recommended that you accept SSL/TLS for incoming mail connections so that account details cannot be intercepted when the relay is enabled. See "SMTP Security" on page 41 for more detailed information on setting up SSL/TLS encryption.

SMTP Banner

Click the **Advanced** button to reveal an option for the SMTP banner. The SMTP banner is exchanged during the HELO session of an SMTP connection. This banner contains identifying information for your 3Com Email Firewall which can be used as information to launch attacks against it. This option allows you to customize the SMTP banner and remove the 3Com Email Firewall's hostname by using the *Domain only* option.

SMTP Security

The 3Com Email Firewall offers a simple mechanism for encrypting mail delivery via SSL (Secure Sockets Layer) and TLS (Transport Layer Security) support. A flexible policy can be implemented to allow other servers and clients to establish encrypted sessions with the 3Com Email Firewall to send and receive mail.

The following types of traffic can be encrypted:

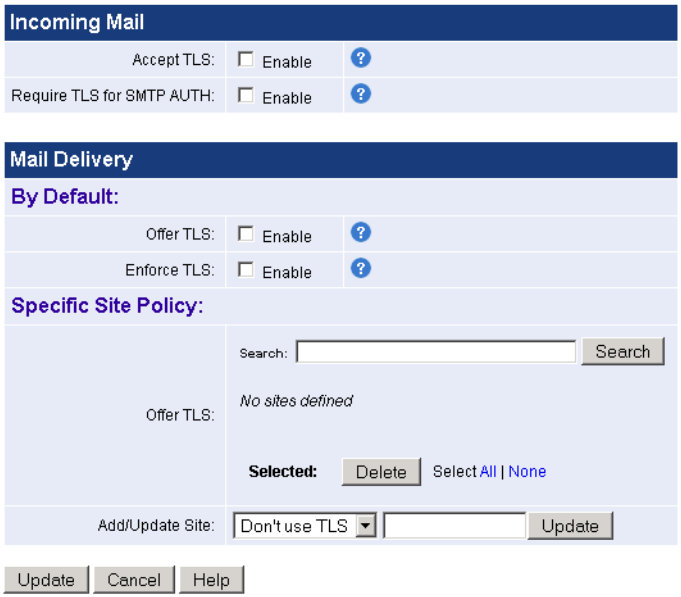
- Server to Server — Used to create an email VPN (Virtual Private Network) and protect company email over the Internet.
- Client to Server — Many email clients support TLS for sending and receiving mail. This allows email messages to be sent confidentiality from desktop to desktop but without the difficulties of implementing other encryption schemes.

Encryption can be enforced between particular systems, such as setting up an email VPN between two 3Com Email Firewalls at remote sites. Encryption can also be set as optional so that users who are concerned about the confidentiality of their messages on the internal network can specify encryption in their mail client when it communicates with the 3Com Email Firewall.

The 3Com Email Firewall supports the use of certificates to initiate the negotiation of encryption keys. The 3Com Email Firewall can generate its own site certificates and it can also import Certificate Authority (CA) signed certificates.

See "SSL Certificates" on page 94 for more information on installing certificates.

Select **Mail Delivery -> SMTP Security** from the menu to enable and configure email encryption.



Incoming Mail

- Accept TLS — Enable this option to accept SSL/TLS for incoming mail connections.
- Require TLS for SMTP AUTH — This value is used to require SSL/TLS when accepting mail for authenticated relay. See the "SMTP Authenticated Relay" section on page 40 for more detailed information.

Mail Delivery

By Default

- Offer TLS — Enable this option to offer remote mail servers the option of using SSL/TLS when sending mail.
- Enforce TLS — Enabling this option will require the validation of a CA-signed certificate when delivering mail to a remote mail server. Failure to do so will result in mail delivery failure.

Specific Site Policy

This option supports the specification of exceptions to the default settings for SSL/TLS. For example, you may need to exempt a mail server from using SSL/TLS because of lack of TLS support.

To exempt a system, specify the IP Address or FQDN (Fully Qualified Domain Name) of the remote mail server in the *Add/Update Site* field. Select **Don't Use TLS** from the dropdown box and click the **Update** button. The exempted mail server will be listed under the *Specific Site Policy*.

TLS options include the following:

- Don't Use TLS — TLS Mail Delivery is never used with the specified system.
- May Use TLS — Use TLS if the specified system supports it.
- Enforce TLS — Deliver to the specified system only if a TLS connection with a valid CA-signed certificate can be established.
- Loose TLS — Similar to *Enforce TLS* but will accept a mismatch between the specified server name and the Common Name in the certificate

See "SSL Certificates" on page 94 for more information on installing certificates.

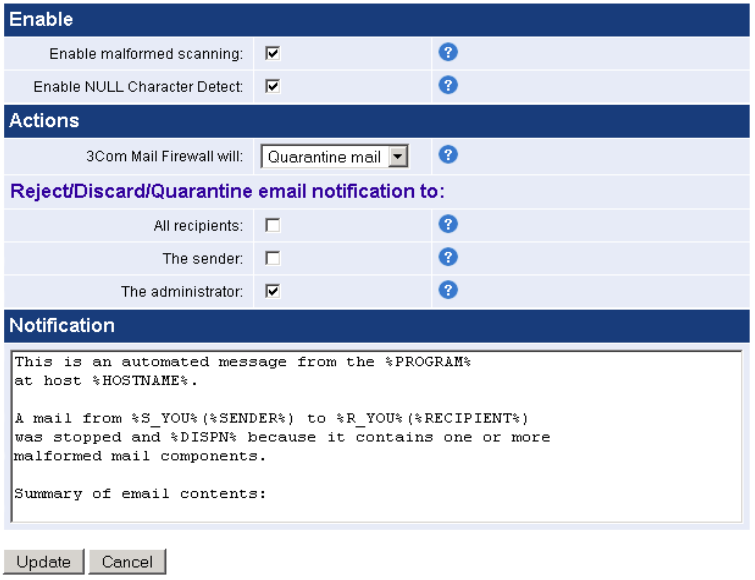
Malformed Email

Many viruses try to elude virus scanners by concealing themselves in malformed messages. The scanning engines cannot detect the attachment and pass the complete message through to an internal server.

Some mail clients try to rebuild malformed messages and may rebuild or activate a virus-infected attachment. Other types of malformed messages are designed to attack mail servers directly. These types of messages are often used in denial-of-service (DoS) attacks.

The 3Com Email Firewall analyzes each message with very extensive integrity checks. Malformed messages are quarantined if they cannot be processed.

Select **Mail Delivery -> Malformed Email** from the menu to configure malformed email checks.



- Enable malformed scanning — Select this option to enable scanning for malformed emails.
- Enable NULL Character Detect — Select this option to enable null character detection. Any messages with null characters in them (a byte value of 0) will be considered a malformed message.

- Actions — Select an action to be performed. Options include:
  - Just log: Log the event and take no further action.
  - Reject mail: The message is rejected with notification to the sending system.
  - Quarantine mail: The message is placed into quarantine.
  - Discard mail: The message is discarded without notification to the sending system.
- Notifications — Notifications for inbound and outbound messages can be enabled for all recipients, the sender, and the administrator, and the notification message can be customized.

See Appendix A "Customizing System Messages" *on* page 125 *for a full list of variables that can be used.*

4 ANTI-SPAM CONFIGURATION

This chapter describes how to configure the Anti-Spam features of your 3Com Email Firewall, and includes the following topics:

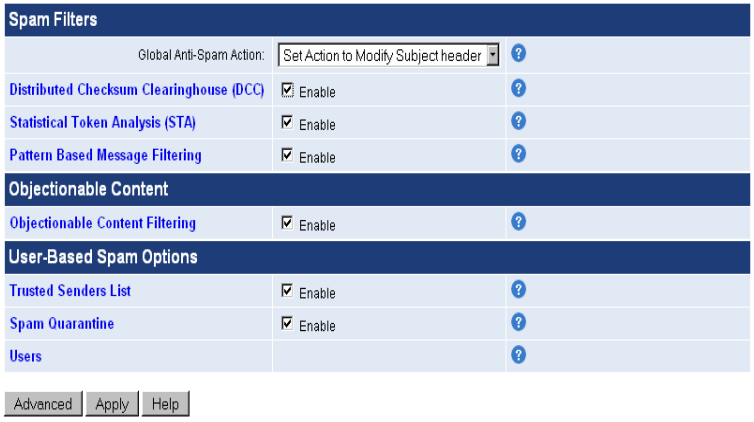
- Anti-Spam Features
- DCC
- STA
- Pattern Based Message Filtering
- Objectionable Content Filtering
- Trusted Senders List
- Spam Quarantine
- Quarantine and Trusted Senders List Users
- Advanced Anti-Spam Options

Anti-Spam Features

The 3Com Email Firewall contains a variety of powerful features to prevent spam messages, including the following:

- Server-based tools such as DCC (Distributed Checksum Clearinghouse), STA (Statistical Token Analysis), Objectionable Content Filtering, and Pattern Based Message Filtering that prevent spam messages from being delivered to an end user's mailbox.
- User-based tools for managing quarantined spam and building trusted senders lists for whitelisting.

Select **Mail Delivery -> Anti-Spam** from the menu to configure the 3Com Email Firewall's Anti-Spam features.



The *Default Anti-Spam Action* defines the type of action to be used for the preselected Anti-Spam features. Possible actions include:

- Disable Anti-Spam — The Anti-Spam features are disabled.
- Set Action to Modify Subject Header — Anti-Spam features are enabled. Messages determined to be spam will have their subject field modified with the text [SPAM].
- Set Action to User-Quarantine Mail — User Spam Quarantine Anti-Spam features are enabled. Messages determined to be spam will be redirected to the User Spam Quarantine. The Action for each feature will be set to *Redirect To*, and the Action data set to the address of this 3Com Email Firewall for quarantine.

CAUTION: *If you set the global Anti-Spam action to User Quarantine Mail, you must ensure you have local Spam Quarantine users configured to accept the messages. If there are no Spam Quarantine users configured, the messages will be rejected.*

See "Quarantine and Trusted Senders List Users" *on* page 67 *for more information on creating Spam Quarantine users.*

DCC

DCC (Distributed Checksum Clearinghouse) is a tool used to identify bulk mail and is based on a number of servers that maintain databases of message checksums. These checksums are derived from numeric values that uniquely identify a message. DCC provides a simple but very effective way to successfully identify spam and control its disposition while updating its database with new spam message types.

Mail users and ISPs all over the world submit checksums of all messages received. The database records how many of each message is submitted. If requested, the DCC server can return a count of how many instances of a message have been received. The 3Com Email Firewall uses this count to determine the disposition of a message.

A DCC server receives no mail, address, headers, or any similar information, but only the cryptographically secure checksums of such information. A DCC server cannot determine the text or other information that corresponds to the checksums it receives. It only acts as a clearinghouse of counts of checksums computed by clients.

You must allow a connection on UDP port 6277 on your network firewall or router to allow communications with a DCC server. If this port is not available, DCC server calls will fail and slow down mail delivery.

Select **DCC** from the **Mail Delivery -> Anti-Spam** menu to configure DCC settings.

- Action — The action can be one of the following:
  - Just log: An entry is made in the log and no other action is taken.
  - Modify Subject Header: The text specified in Action Data will be inserted into the message subject line.
  - Add header: An "X-" mail header will be added as specified in the Action Data.

- Redirect to: The message will be delivered to the mail address specified in Action Data.
- Reject mail: The mail will not be accepted and the connecting mail server is forced to return it.
- BCC (Blind Carbon Copy): The message will be copied to the mail address specified in Action Data.

- Action data — Depending on the specified action:
  - Modify Subject Header: The specified text will be inserted into the subject line, such as [BULK].
  - Add header: A message header will be added with the specified text, such as [BULK].
  - Redirect to: Send the message to a mailbox such as *spam@example.com*.

STA

STA (Statistical Token Analysis) is a sophisticated method of identifying spam based on statistical analysis of mail content. Simple text matches can lead to false positives because a word or phrase can have many meanings depending on the context. STA provides a way to accurately measure how likely any particular message is to be spam without having to specify every word and phrase.

STA achieves this by deriving a measure of a word or phrase contributing to the likelihood of a message being spam. This is based on the relative frequency of words and phrases in a large number of spam messages. From this analysis, it creates a table of "discriminators" (words associated with spam) and associated measures of how likely a message is spam.

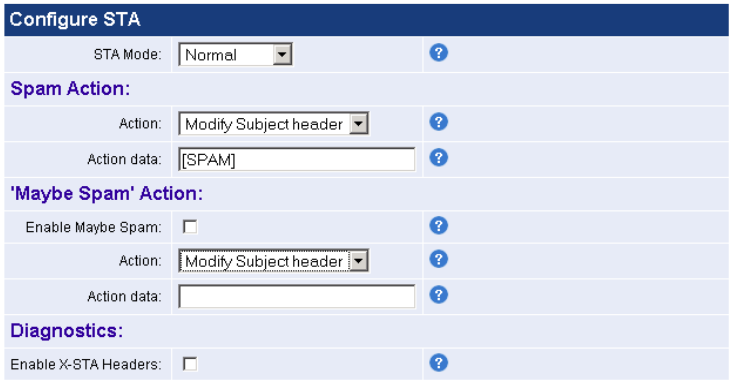
When a new incoming message is received, STA analyzes the message, extracts the discriminators (words and phrases), finds their measures from the table, and aggregates these measures to produce a spam metric for the message between 1 and 100.

STA uses three sources of data to build its run-time database:

- The initial database tables based on analysis of known spam.
- Tables derived from an analysis of local legitimate mail. This is referred to as "training."

- Mail identified as "bulk" by DCC is also analyzed to provide an example of local spam.

Select **STA** from the **Mail Delivery -> Anti-Spam** menu to configure STA settings.



- STA Mode — Use one of the following three modes for STA:
  - Normal: This is the default mode and is recommended in most cases. The STA upper threshold is set to 85, and the lower threshold to 65. Any message with a metric 85 or above will be considered spam. A metric between 85 and 65 will be considered Maybe Spam, and will trigger an action if you have the Maybe Spam option enabled. A metric lower than 65 is considered legitimate mail.
  - Aggressive: Increases STA's aggressiveness to ensure more spam is caught, but also increases the possibility of false positives.The STA upper threshold is set to 80, and the lower threshold to 50. Any message with a metric 80 or above will be considered spam. A metric between 80 and 50 will be considered Maybe Spam, and will trigger an action if you have the Maybe Spam option enabled. A metric lower than 50 is considered legitimate mail.
  - Lenient: Reduces the possibility of false positives, but more spam may get through. The STA upper threshold is set to 90, and the lower threshold to 80. Any message with a metric 90 or above will be considered spam. A metric between 90 and 80 will be considered Maybe Spam, and will trigger an action if you have the Maybe Spam option enabled. A metric lower than 80 is considered legitimate mail.

Spam Action Specify an action when STA flags a message as spam.

- Action — The action can be one of the following:
  - Just log: An entry is made in the log and no other action is taken.
  - Modify Subject Header: The text specified in Action Data will be inserted into the message subject line.
  - Add header: An "X-" mail header will be added as specified in the Action Data.
  - Redirect to: The message will be delivered to the mail address specified in Action Data.
  - Reject mail: The mail will not be accepted and the connecting mail server is forced to return it.
  - BCC: The message will be copied to the mail address specified in Action Data.
- Action data — Depending on the specified action:
  - Modify Subject Header: The specified text will be inserted into the subject line, such as [SPAM].
  - Add header: A message header will be added with the specified text, such as [SPAM].
  - Redirect to: Send the message to a mailbox such as *spam@example.com*.

Maybe Spam Action This features allows you to take action on messages that STA identifies as "maybe spam" which indicates it could be spam but may also be legitimate mail. A message is considered to be "maybe spam" if its metric is between the upper and lower thresholds as configured by your STA mode (Normal, Aggressive, Lenient).

- Enable Maybe Spam — Select the check box to enable actions for "maybe" spam.
- Action — The action can be one of the following:
  - Just log: An entry is made in the log, and no other action is taken.
  - Modify Subject Header: The text specified in Action Data will be inserted into the message subject line.
  - Add header: An "X-" mail header will be added as specified in the Action Data.

- Redirect to: The message will be delivered to the mail address specified in Action Data.
- Reject mail: The mail will not be accepted and the connecting mail server is forced to return it.
- BCC: The message will be copied to the mail address specified in Action Data.

- Action data — Depending on the specified action:
  - Modify Subject Header: The specified text will be inserted into the subject line, such as [SPAM].
  - Add header: A message header will be added with the specified text, such as [SPAM].
- Redirect to: Send the message to a mailbox such as *spam@example.com*.

Diagnostics

- Enable X-STA Headers — This setting inserts X-STA headers into all messages. These are not visible to the user (although they can be filtered in most mail clients), but can be used to gather information on why mail is processed in a particular way.

  The following headers will be inserted:
  - X-STA-Metric: The "score" assigned by STA, such as 95, which would indicate a spam message.
  - X-STA-NotSpam: Indicates the words with the highest non-spam value found in the message.
  - X-STA-Spam: Indicates the words with the highest spam value found in the message.

STA Training

The STA training section displays statistics of all mail analyzed by the 3Com Email Firewall.

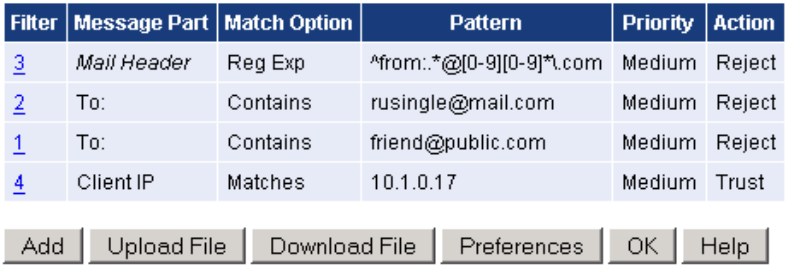
Click the **Rebuild STA** button to rebuild the STA database. The STA run-time engine is built and rebuilt at 12 hour intervals using several sources such as the supplied spam data, the DCC spam (if enabled), and local training. Since the database is not built for the first time until 12 hours after installation, you can use this button to immediately rebuild the STA database.

Click the **Delete Training** button to delete all training material if your 3Com Email Firewall has been misconfigured and starts to treat legitimate mail as spam or vice versa.

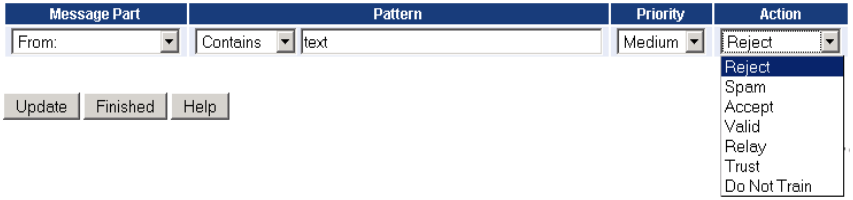
Pattern Based Message Filtering

Pattern Based Message Filtering is the primary tool for whitelisting and blacklisting messages. An administrator can specify that mail is rejected or whitelisted according to the contents of the message envelope, message header (such as the sender, recipient, subject), and body text.

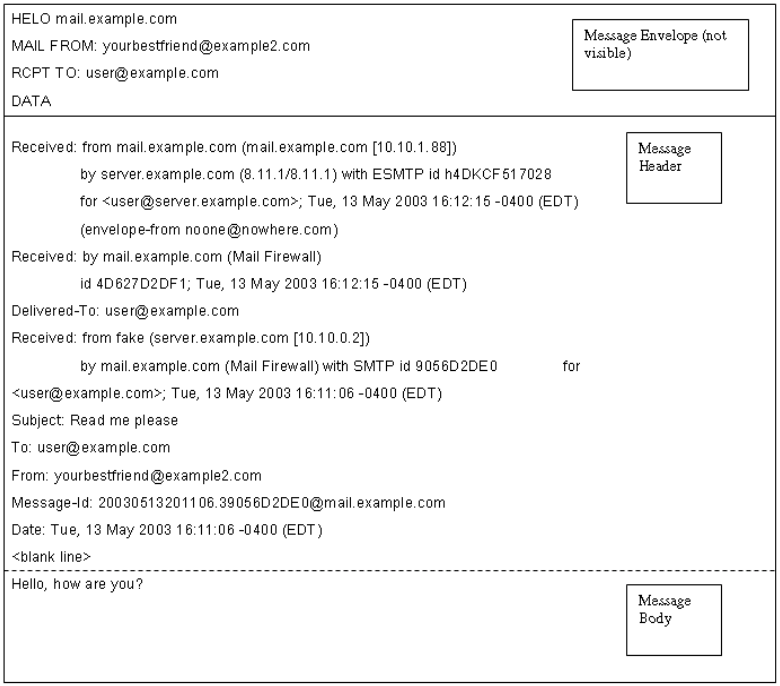
Select **Pattern Based Message Filtering** from the **Mail Delivery -> Anti-Spam** menu to configure your PBMF rules.



Some default PBMF rules are provided and more can be added by clicking the **Add** button.



Message Part Select a *Message Part* from the dropdown list. The following diagram and sections explain each part of the mail message.


HELO mail.example.com
MAIL FROM: yourbestfriend@example2.com
RCPT TO: user@example.com
DATA
Message Envelope (not visible)
Received: from mail.example.com (mail.example.com [10.10.1.88])
by server.example.com (8.11.1/8.11.1) with ESMTP id h4DKCF517028
for <user@server.example.com>; Tue, 13 May 2003 16:12:15 -0400 (EDT)
(envelope-from noone@nowhere.com)
Received: by mail.example.com (Mail Firewall)
id 4D627D2DF1; Tue, 13 May 2003 16:12:15 -0400 (EDT)
Delivered-To: user@example.com
Received: from fake (server.example.com [10.10.0.2])
by mail.example.com (Mail Firewall) with SMTP id 9056D2DE0 for
<user@example.com>; Tue, 13 May 2003 16:11:06 -0400 (EDT)
Subject: Read me please
To: user@example.com
From: yourbestfriend@example2.com
Message-Id: 20030513201106.39056D2DE0@mail.example.com
Date: Tue, 13 May 2003 16:11:06 -0400 (EDT)
<blank line>
Message Header
Hello, how are you?
Message Body

Message Envelope Parameters

These parameters will not be visible to the user. They are the "handshake" part of the SMTP protocol. You will need to look for these in the transport logs or have other knowledge of them.

- <<Mail Envelope>> — This parameter allows for a match on any part of the message envelope which includes the HELO, Client IP and Client Host.
- HELO — This field is easily faked and is not recommended for use in spam control. It may be useful in whitelisting a source of mail. Example: *mail.example.com*.
- Client IP — This field will be accurately reported and may be reliably used for both blacklisting and whitelisting. It is the IP address of the system initiating the SMTP connection. Example: *174.17.19.241*.
- Client Host — This field will be accurately reported and may be reliably used for both blacklisting and whitelisting. Example: *mail.example.com*.

The following envelope parameters (*Envelope Addr, Envelope To and Envelope From*) may be visible if your client supports reading the message source. They can also be found in the transport logs. Other header fields may be visible as supported by the mail client.

- Envelope Addr — This matches on either the Envelope To or Envelope From. These fields are easily faked and are not recommended for use in spam control. They may be useful in whitelisting a source of mail. Example: *user@example.com*.
- Envelope To — This field is easily faked, and is not recommended for use in spam control. It may be useful in whitelisting a source of mail. Example: *user@example.com*.
- Envelope From — This field is easily faked, and is not recommended for use in spam control. It may be useful in whitelisting a source of mail. Example: *user@example.com*.

Message Header Parameters

Spammers will typically enter false information into these fields and, except for the Subject field, they are usually not useful in controlling spam. These fields may be useful in whitelisting certain users or legitimate source of email.

- <<Mail Header>> — This parameter allows for a match on any part of the message header.
- <<Recipient>> — This parameter matches the To: or CC: fields.
- CC:
- From:
- Message-ID:
- Received:
- Reply-to:
- Sender:
- Subject:
- To:

Message Body Parameters

- <<Raw Mail Body>> — This parameter allows for a match on any part of the encoded message body. This encoded content includes Base64, MIME, and HTML. Since messages are not decoded, a simple text match may not work. Use <<Mail Content>> for text matching on the decoded content.
- <<Mail Content>> — This parameter allows for a match on the visible decoded message body.

STA Token

STA tokens can also be selected for pattern based message filters. This allows you to match patterns for common spam words that could be hidden or disguised with fake or invisible HTML text comments that would not be caught by a normal pattern filter. For example, STA extracts the token "viagra" from the text "vi<spam>ag<spam>ra" and "v.i.a.g.r.a.".

Match Option The match option looks for the specified text in each line. You can specify one of the following:

- Contains — Looks for the text to be contained in a line or field. This allows for spaces or other characters that may make an exact match fail.
- Ends with — Looks for the text at the end of the line or field (no characters, spaces and so on, between the text and the non-printed end-of-line character.)
- Matches — The entire line or field must match the text.
- Starts with — Looks for the text at the start of the line or field (no characters between the text and the start of line.)
- Reg Exp — Use a Regular Expression to define a pattern that matches various text strings.

Pattern Enter the pattern you wish to search for.

Priority Select a priority for the filter (*High, Medium, Low*). The entire message is read before making the decision. If a message matches multiple filters, the filter with the highest priority will be used. If more than one matched filter has the highest priority, the filter with the strongest action will be used, in order, from highest priority to lowest (*Spam, Reject, Trust, Relay, Valid, Accept)*. If more than one matched rule has the highest priority and highest action, then the filter with the highest rule number will be used.

Action When a rule has been triggered, the specified action is carried out:

- Reject — Mail is received, then rejected before the close of an SMTP session.
- Spam — Mail is received, then trained as spam for STA, and then rejected.
- Accept — Mail is delivered normally and not trained by STA, or marked as spam or bulk. Attempted relays are rejected.
- Valid — Mail is delivered normally and trained as valid by STA. Attempted relays are rejected.
- Relay — Relay is enabled for this mail. Mail is not trained by STA.
- Trust — Relay is enabled for this mail. Mail is trained as valid by STA.

- Do Not Train — Do not use the message for STA training purposes. This option will not override other PBMF's if it applies to the same message.
- BCC — Send a blind carbon copy mail to the mail address specified in Action Data. This option only appears if you have a BCC Email Address set up in the *Preferences* section.

Upload or Download File

You can create a list of PBMF rules and upload them together in one file.

The file must contain comma or tab separated entries in the form:

[Section],[type],[pattern],[action],[priority(seq)],[rulenumber]

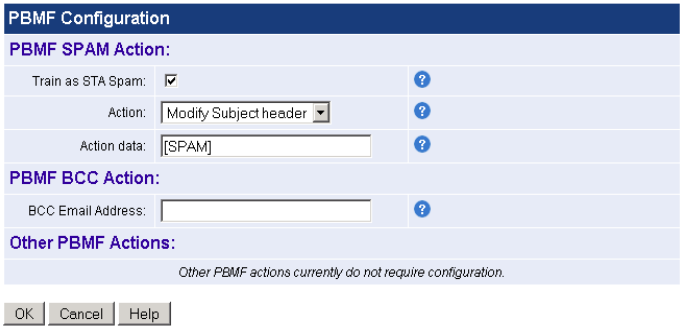
For example:

to:,contains,user@example.com,reject,medium,1

The file (*pbmf.csv*) should be created in csv file format using Excel, Notepad or other Windows text editor. It is recommended that you download the PBMF file first by clicking **Download File**, edit it as required, and upload it using the **Upload File** button.

PBMF Preferences

Click the **Preferences** button to set your preferences for any spam PBMF's.



- Train as STA Spam — Select this option to allow any mail that triggers an action to be trained as spam for STA purposes.
- Action — Specify one of the following actions:
  - Just log: An entry is made in the log and no other action is taken.

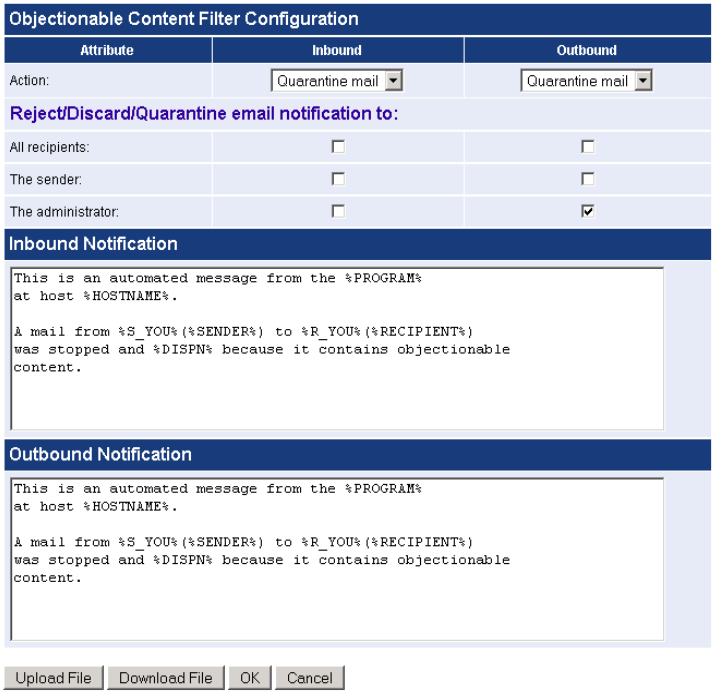
- Modify Subject Header: The text specified in Action Data will be inserted into the message subject line.
- Add header: An "X-" mail header will be added as specified in the Action Data.
- Redirect to: The message will be delivered to the mail address specified in Action Data.
- Reject mail: The mail will not be accepted and the connecting mail server is forced to return it.
- BCC: Send a blind carbon copy mail to the mail address specified in Action Data.

- Action data — Depending on the specified action:
  - Modify Subject Header: The specified text will be inserted into the subject line, such as [SPAM].
  - Add header: A message header will be added with the specified text, such as [SPAM].
  - Redirect to: Send the message to a mailbox such as *spam@example.com*.
- PBMF BCC Action — Send a blind carbon copy of the message to the address specified. This is a separate action from the PBMF spam actions.

Objectionable Content Filtering

The Objectionable Content Filter defines a list of key words that will cause a message to be blocked if any of those words appear in the message.

Select **Objectionable Content Filtering** from the **Mail Delivery -> Anti-Spam** menu to configure the filter.



Actions

You can set actions for both inbound and outbound messages. The following actions can be set:

- Just log: Log the event and take no further action.
- Reject mail: The message is rejected with notification to the sending system.
- Quarantine mail: The message is placed into quarantine.
- Discard mail: The message is discarded without notification to the sending system.

Notifications

Notifications for inbound and outbound messages can be enabled for all recipients, the sender, and the administrator. The content for the *Inbound* and *Outbound* notification can be customized.

See Appendix A "Customizing System Messages" *on* page 125 *for a full list of variables that can be used.*

Upload and Download Filter List

A predefined list of objectionable words is included with the 3Com Email Firewall. To customize the list and to add or remove words, click **Download File** to download the list to a local system.

Use a text editor to edit the file using one word or phrase per line. When finished, upload the file by clicking the **Upload File** button.

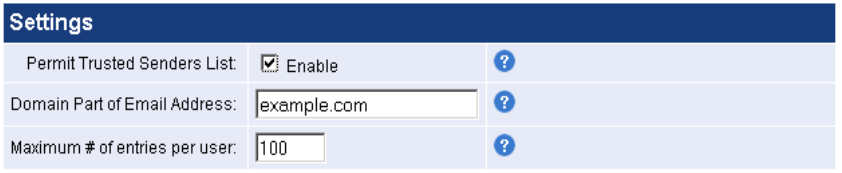
Trusted Senders List

The Trusted Senders List allows users to define specific email addresses that are considered "trusted" and bypass the 3Com Email Firewall's Anti-Spam controls (DCC, STA, RBL, and PBMF "Spam").

If the action for an Anti-Spam feature is set to "Reject", it cannot be bypassed by the Trusted Senders List. Additionally, the Trusted Senders List only applies to PBMF "Spam" messages with a low priority.

Local 3Com Email Firewall users can log in and create their own list of Trusted Senders.

The Trusted Senders List must first be enabled globally by the administrator by clicking on **Trusted Senders List** in the **Mail Delivery -> Anti-Spam** menu.



- Enable Trusted Senders List — The Trusted Senders List must be enabled by the administrator before individual users can add addresses to their list.
- Domain Part of Email Address — Enter the mail domain part of the local user's email address for the domain you are receiving mail for.

- Maximum number of entries per user — Enter a maximum number of list entries for each user.

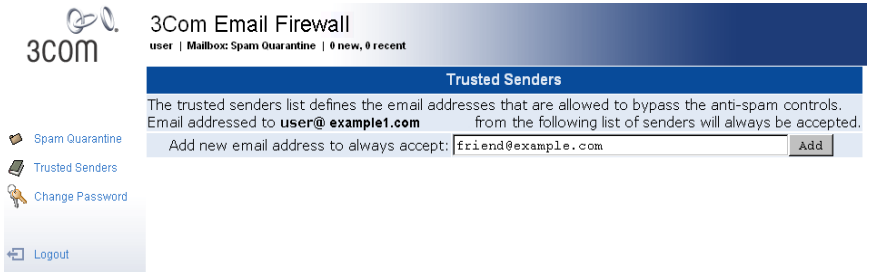
Adding Trusted Senders

When the Trusted Senders List option is enabled globally, local 3Com Email Firewall users can log in and add their own addresses using the same interface as they use for checking the Spam Quarantine.

See "Quarantine and Trusted Senders List Users" on page 67 for details on how to add local users to the system.

Log in to the 3Com Email Firewall and select **Trusted Senders** in the left menu.

Enter an email address and then click the **Add** button. The specified address will bypass the 3Com Email Firewall's Anti-Spam controls when they send you messages.


3Com Email Firewall
user | Mailbox: Spam Quarantine | 0 new, 0 recent
Trusted Senders
The trusted senders list defines the email addresses that are allowed to bypass the anti-spam controls.
Email addressed to user@ example1.com from the following list of senders will always be accepted.
Add new email address to always accept: friend@example.com
Add
Spam Quarantine
Trusted Senders
Change Password
Logout

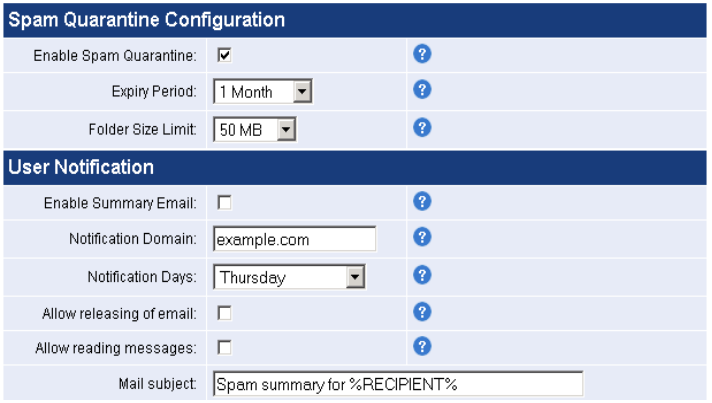
Spam Quarantine

The Spam Quarantine contains quarantined mail messages for each local user on the 3Com Email Firewall.

For each Anti-Spam feature (DCC, STA, and so on) that you want to use the user Spam Quarantine, you must set the Action to *Redirect To*, and the Action Data to the 3Com Email Firewall address such as *mail.example.com*.

This will redirect the message to the spam quarantine where it will be placed in a folder for that particular user. Users can log in to the 3Com Email Firewall and manage their quarantined spam. Messages can be viewed, returned to the inbox, or deleted.

Select **Spam Quarantine** from the **Mail Delivery -> Anti-Spam** menu.



Spam Quarantine Configuration

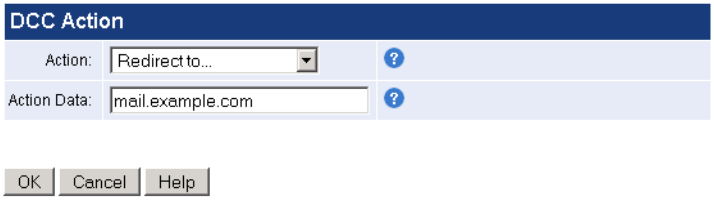
- Enable Spam Quarantine — Select the check box to enable the spam quarantine.
- Expiry Period — Select an expiry period for mail in each quarantine folder. Any mail quarantined for longer than the specified value will be deleted.
- Folder Size Limit — Set a value, in megabytes, to limit the amount of stored quarantined mail in each quarantine folder.

User Notification

- Enable Summary Email — Select the check box to enable a summary email notification that alerts users to mail that has been placed in their quarantine folder.
- Notification Domain — Enter the domain for which notifications are sent to. This is typically the FQDN (Fully Qualified Domain Name) of the email server.
- Notification Days — Select the specific Notification Days to send the summary.
- Allow releasing of email — When enabled, a link labelled "Not Spam" is inserted into the spam summary email so that the user may release the message to their inbox and additionally add the sender to the their trusted senders list.
- Allow reading messages — When enabled, a link is inserted into the spam summary message to allow the user to read the original message.
- Mail Subject — Enter a subject for the notification email.
- Mail Content Preamble — Customize the preamble that will appear in the message.

Set Redirect Action for Anti-Spam Features

For each Anti-Spam feature (DCC, STA, and so on) that you want to use the user Spam Quarantine, you must set the Action to *Redirect To*, and the Action Data to the 3Com Email Firewall address such as *mail.example.com*.



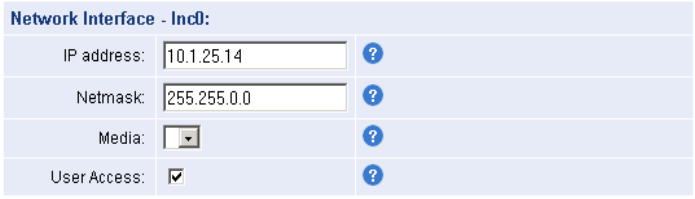
CAUTION: *You must ensure you have local Spam Quarantine users configured to accept the quarantined message. If there are no Spam Quarantine users configured, the message will be rejected.*

See "Quarantine and Trusted Senders List Users" *on* page 67 *for more information on creating Spam Quarantine users.*

Enabling User Access on a Network Interface

You must enable User Access on the network interface to allow users to login to the Spam Quarantine via that interface.

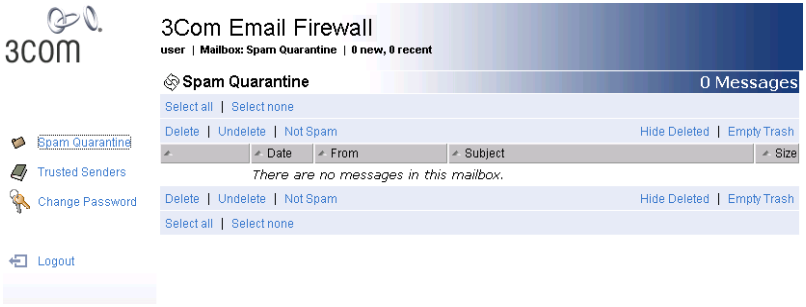
Select **System Config -> Network Settings** and go to the *Network Interface* section.



Select the **User Access** check box to allow access to the Spam Quarantine via this interface. Click **Apply** to save the network settings.

Examining the Quarantine

Local Email Firewall users can log in and examine the messages in their Spam Quarantine. Messages in the quarantine can be released back into the user's Inbox by clicking the **Not Spam** link.

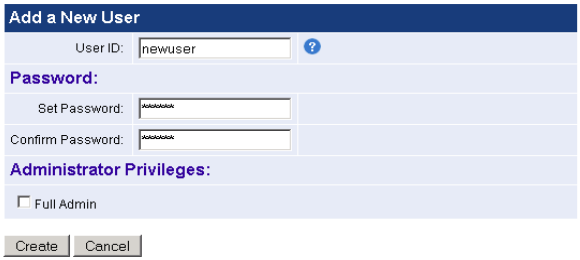


Quarantine and Trusted Senders List Users

You must add local users to the 3Com Email Firewall if you require the ability for users to view the Spam Quarantine or configure their Trusted Senders Lists.

Select **System Config -> Users** from the menu.

Click the **Add a New User button** to add a new user to the system.



Enter a user ID and a password.

If this user will be an additional administrator for this Email Firewall, select the **Full Admin** option in the *Administrator Privileges* section.

Upload and Download User Lists

You can upload lists of users using comma or tab separated text files. You can specify the login ID, password, email address, and disk quota in megabytes. Use the following format:

[login],[password],[email address],[quota]

For example,

user,ajg7rY,user@example.com,0

The file (*user.csv*) should be created in csv file format using Excel, Notepad or other Windows text editor. It is recommended that you download the user list file first by clicking **File Download**, editing it as required, and then uploading it using the **File Upload** button.

Enabling User Access on a Network Interface

You must enable User Access on the network interface to allow users to log in via that interface.

Select **System Config -> Network Settings** and go to the *Network Interface* section.

Select the **User Access** check box to allow local access to the Spam Quarantine and Trusted Senders List via this interface. Click **Apply** to save the network settings.

Advanced Anti-Spam Options

Click the **Advanced** button to reveal the following advanced Anti-Spam options.

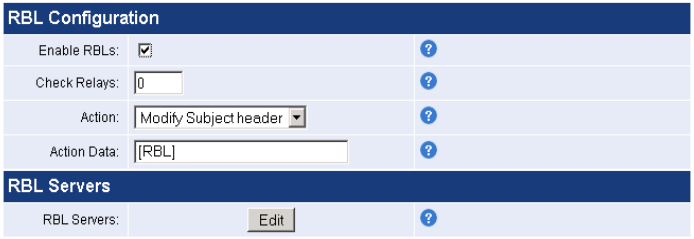
RBL (Realtime Blackhole List)

RBLs contain the addresses of known sources of spam and are maintained by both commercial and non-commercial organizations.

The RBL mechanism is based on DNS. Every server that attempts to connect to the 3Com Email Firewall will be looked up on the specified RBL servers using DNS. If the server is blacklisted, then the server is considered an origin of known spam and the connection dropped.

Note the following considerations when using RBL:

- If the RBL server is not available, the DNS request times out. This may affect performance and requires monitoring for timed-out connections.
- If a message that you want to receive is blocked by an RBL, add an item to the *Pattern Based Message Filtering* list to "Trust" (to train for STA) or "Accept" (not train for STA) this message.



- Enable RBLs — Select this check box to enable RBLs.
- Check Relays — The Check Relays setting deals with spammers who are relaying their messages through an intermediate server. The information about the originating server is carried in the headers of the message which is checked against the RBL. For example, set *Check Relays* to "2" to look for the last two relays.
- Action — Specify one of the following actions:
  - Just log: An entry is made in the log and no other action is taken.
  - Modify Subject Header: The text specified in Action Data will be inserted into the message subject line.

- Add header: An "X-" mail header will be added as specified in the Action Data.
- Redirect to: The message will be delivered to the mail address specified in Action Data.
- Reject mail: The mail will not be accepted and the connecting mail server is forced to return it.
- BCC: The message will be copied to the mail address specified in Action Data.

- Action data — Depending on the specified action:
  - Modify Subject Header: The specified text will be inserted into the subject line, such as [RBL].
  - Add header: A message header will be added with the specified text, such as [RBL].
  - Redirect to: Send the message to a mailbox such as *spam@example.com*.
- RBL Servers — Click the **Edit** button to edit your RBL server addresses.

Mail Access/Filtering

In the *Mail Access/Mail Filtering* settings, you can specify patterns to match for on incoming connections and configure an appropriate action. The maximum number of recipients and the maximum size of a message can also be configured.

See "Mail Access/Filtering" on page 37 for more detailed information on configuring Mail Access/Filtering settings.

Anti-Spam Header

This feature adds a header to scanned email messages displaying the results of the 3Com Email Firewall's Anti-Spam processing.

The header output is similar to the following:

```
X-AntiSpam: sta:false/0/020,dcc:off,rbl:off,wlbl:none
```

5 REPORTING

This chapter describes the reporting features of the 3Com Email Firewall, and includes the following topics:

- Generating Reports
- System Logs
- Email History
- System History
- Configure History Settings

Generating Reports

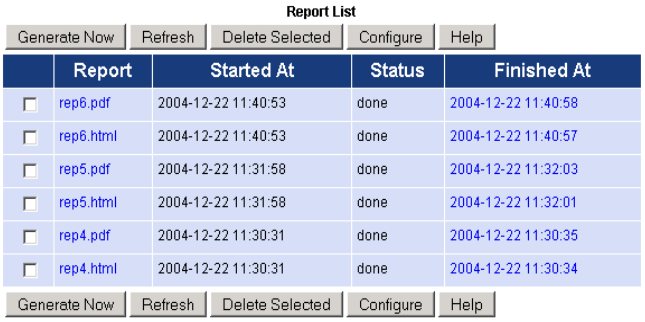
The 3Com Email Firewall's reporting features provide a comprehensive range of informative reports including the following:

- Traffic Summary
- System Health
- Top Mailbox Disk Users
- Spam Statistics
- Virus Reports
- Email History
- System Events History

The reports are derived from information written to the various systems logs and then stored in the database. Reports are stored on the system for online viewing and can also be emailed automatically to specified users. Reports can be generated on demand and at scheduled times. Reports can also be filtered to provide reporting on only mail domains, user groups, or specific hosts.

Administrators can specify which data is to be included in each report, how it is to be displayed, the order of data, and the number of entries to report, such as "Top 10 Disk Space Users".

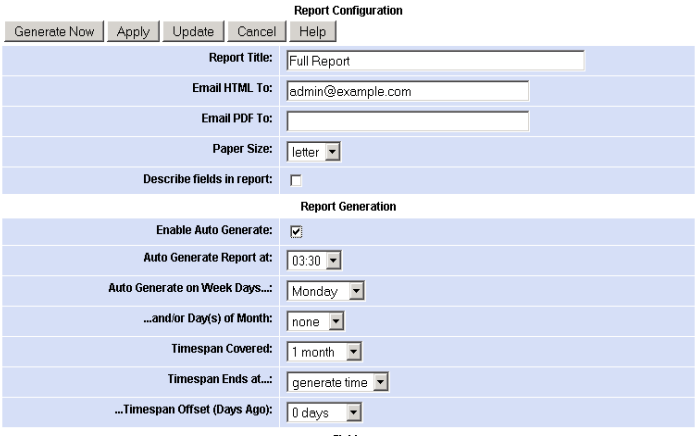
Select **Reporting** from the menu to view and configure reports.



To view a previously generated report, click on the report name. To configure a report, click the **Configure** button. Click **Generate Now** to immediately generate a report.

Report Configuration

Click the **Configure** button to set up a new report.



- Report Title — Title to display at the top of the report.
- Email To (HTML, PDF) — Specify an email address, such as *admin@example.com*. Use a comma-separated list if you wish to distribute the report to multiple users.

- Paper Size — For PDF format, select the paper size such as Letter, A4, or Legal.
- Describe fields in report — Select this option to include a short description of each field in the report.

Report Generation

- Enable Auto Generate — Select this check box to automatically generate reports.
- Auto Generate Report at — Select the time to generate the report.
- Auto Generate on Week Days… — Choose the days of the week to generate the report.
- ...and/or Day(s) of Month — Choose specific days of the month to generate the report.
- Timespan Covered — Select the timespan covered for this report.
- Timespan Ends at… — Select the end of the timespan. It is recommended to set the timespan end time a few hours prior to report generation to allow all deferred mail to be finalized.
- ...Timespan Offset (Days Ago) — Select the number of days to offset the timespan. This amount of time is subtracted before setting the timespan.

Click the **Generate Now** button to generate a report on demand using the specified settings. This will also automatically email the report to the specified address.

To generate a report daily at 2.00am for the previous day (up to 11:00pm) use the following settings:

Auto Generate Report at: 02:00
Auto Generate on Week Days:All
Timespan covered:1 day
Timespan ends at:23:00
Timespan offset:0 days

Report Fields

The *Fields* section allows you to choose which fields or items of information you wish to include in the report. You can include or exclude fields as required. Use the *Limit* column to limit the number of items for that field, such as listing the "Top Ten" viruses.

Included	Field ID	Title in Report	Order	Page Break	Limit
☑	system name	System Name	10	no	
☑	date time	Date and Time	20	no	
☑	version	Software Version	30	no	
☑	timespan	Timespan	40	no	
☑	uptime	Uptime	50	no	
☑	filter summary	Filters Applied	60	no	
☐	head comment	head comment	90	no	
☑	traffic blocking	Traffic and Filtering Summary	100	no	
☑	blocking pie chart	Traffic Blocking Ratios	110	no	
☑	total traffic received	Total Traffic Received	120	no	
☑	total traffic sent	Total Traffic Sent	125	no	
☑	total received message size	Total Received Message Size	130	no	
☑	total sent out message size	Total Sent Out Message Size	135	no	
☑	processing time	Message Processing Time	150	no	
☑	spam metrics	Spam Metric Frequency	160	no	100
☑	top virus	Top Virus List	170	no	10

Table 3 Report Field Descriptions

Field	Description
System name	The system host name, such as *mail.example.com*.
Date time	Date and time of report generation.
Version	Software version.
Timespan	Period covered by report.
Uptime	How long the system has been running since the last reboot.
Filter summary	A summary of the filters applied to this report.
Head comment	Freeform comment that you may enter.
Traffic blocking	A table showing the number of messages caught by each method over the preceding hour, day, week, month, and report timespan.

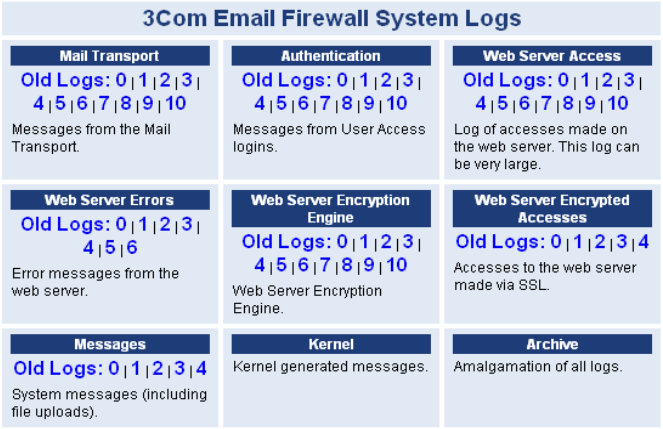
Field	Description
Blocking pie chart	A pie chart of the same data as the right hand column of Traffic Blocking (timespan).
Total traffic Received	Graphs of the number of messages received per hour over the reporting period (timespan).
Total traffic sent	Graphs of the number of messages sent per hour over the reporting period (timespan).
Total received message size	Total message size of incoming messages per hour.
Total sent out message size	Total message size of outgoing messages per hour.
Processing time	The average time a message waits between initial handshake and disposition, including RBL/DCC lookups if any. Messages that are deferred are not included.
Spam metrics	Graph of the number of messages per STA assigned spam metric (0 - 100).
Top virus	List of the top viruses found.
Recent virus list	List of the most recent viruses found.
Top PBMFs	List of the top pattern based message filters.
Top forbidden attachments	List of the top forbidden attachments caught by attachment control.
Recent forbidden attachments	List of the most recent forbidden attachments caught by attachment control.
Disk usage	Shows disk usage by partition.
Disk load	Graph of average disk load (MB/s) over the reporting period.
CPU load	Graph of average CPU load (number of waiting processes) over the reporting period.
NIC load	Graph for each active network interface load (Bytes/hour) for the reporting period.
Swap usage	Swap file usage.
Paging	Paging usage.
Top spam quarantine sizes	Lists the top users based on the size of their spam quarantine in MB.
Active mail queue	Graph showing number of queued messages (as sampled every 5 minutes) over the reporting period.
Deferred mail queue	Graph showing maximum number of messages (as sampled every 5 minutes) in the deferred queue over the reporting period.

Field	Description
Top senders	The top sender (judged by Envelope from, not Header from) during the report timespan, sorted by number of messages. If the title contains one or more comma characters, the list will be restricted to those senders which include any string after the first comma. The limit parameter in the report configuration sets the maximum number listed.
Top sending hosts	The top sending hostnames (in FQDN format) during the report timespan, sorted by number of messages. If the title contains one or more comma characters, the list will be restricted to those sender FQDNs which include any string after the first comma. The limit parameter in the report configuration sets the maximum number listed.
Top recipients	The top recipients during the report timespan, sorted by number of messages. The sum of the message sizes is also listed. If the title contains one or more comma characters, the list will be restricted to those recipients which include any string after the first comma. The limit parameter in the report configuration sets the maximum number listed.
DCC Servers	Graph showing the average round trip, in seconds, to the preferred DCC server over the reporting period.
RBL Servers	Graph showing the round trip, in seconds, to the RBL servers over the reporting period. The value is averaged over all enabled RBL servers.
End comment	Comment text.
Extra comment	Extra comment text.

System Logs

The system logs provide detailed information on all mail transport and system related events.

Select **Reporting -> System Logs** from the menu to view the log files.


3Com Email Firewall System Logs
Mail Transport
Old Logs: 0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10
Messages from the Mail Transport.
Authentication
Old Logs: 0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10
Messages from User Access logins.
Web Server Access
Old Logs: 0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10
Log of accesses made on the web server. This log can be very large.
Web Server Errors
Old Logs: 0 | 1 | 2 | 3 | 4 | 5 | 6
Error messages from the web server.
Web Server Encryption Engine
Old Logs: 0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10
Web Server Encryption Engine.
Web Server Encrypted Accesses
Old Logs: 0 | 1 | 2 | 3 | 4
Accesses to the web server made via SSL.
Messages
Old Logs: 0 | 1 | 2 | 3 | 4
System messages (including file uploads).
Kernel
Kernel generated messages.
Archive
Amalgamation of all logs.

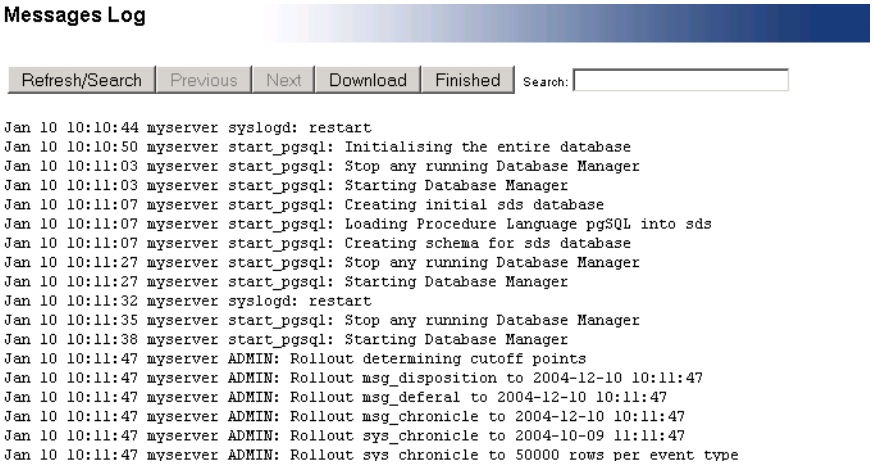
The **Mail Transport** log is the most important log to monitor because it contains a record of all mail processed by the 3Com Email Firewall.

Other logs include:

- Authentication — Contains messages from Spam Quarantine logins.
- Web Server Access — A log of access to the web server.
- Web Server Errors — Contains error messages from the web server.
- Web Server Encryption Engine — Contains messages for the web server encryption engine.
- Web Server Encrypted Accesses — A log of SSL web server access.
- Messages — Contains system messages, including file uploads.
- Kernel — A log of kernel generated messages.
- Archive — This option allows you to view an amalgamation of all the logs.

Viewing Log Details

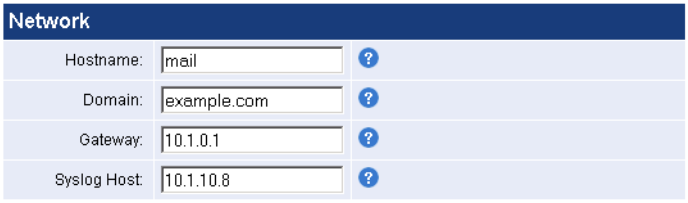
Select a specific log to view, search, and download its detailed entry information.


Messages Log
Refresh/Search
Previous
Next
Download
Finished
Search:
Jan 10 10:10:44 myserver syslogd: restart
Jan 10 10:10:50 myserver start_pgsql: Initialising the entire database
Jan 10 10:11:03 myserver start_pgsql: Stop any running Database Manager
Jan 10 10:11:03 myserver start_pgsql: Starting Database Manager
Jan 10 10:11:07 myserver start_pgsql: Creating initial sds database
Jan 10 10:11:07 myserver start_pgsql: Loading Procedure Language pgSQL into sds
Jan 10 10:11:07 myserver start_pgsql: Creating schema for sds database
Jan 10 10:11:27 myserver start_pgsql: Stop any running Database Manager
Jan 10 10:11:27 myserver start_pgsql: Starting Database Manager
Jan 10 10:11:32 myserver syslogd: restart
Jan 10 10:11:35 myserver start_pgsql: Stop any running Database Manager
Jan 10 10:11:38 myserver start_pgsql: Starting Database Manager
Jan 10 10:11:47 myserver ADMIN: Rollout determining cutoff points
Jan 10 10:11:47 myserver ADMIN: Rollout msg_disposition to 2004-12-10 10:11:47
Jan 10 10:11:47 myserver ADMIN: Rollout msg_deferal to 2004-12-10 10:11:47
Jan 10 10:11:47 myserver ADMIN: Rollout msg_chronicle to 2004-12-10 10:11:47
Jan 10 10:11:47 myserver ADMIN: Rollout sys_chronicle to 2004-10-09 11:11:47
Jan 10 10:11:47 myserver ADMIN: Rollout sys_chronicle to 50000 rows per event type

Configuring a Syslog Server

Logs can also be forwarded to a *syslog* server which is a host that collects and stores log files from many sources.

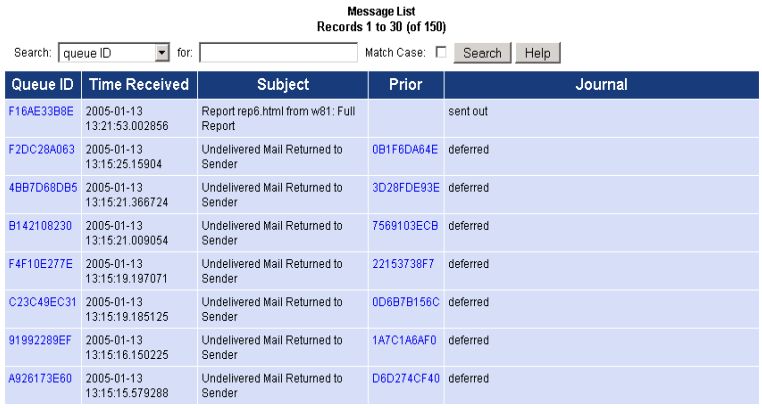
You can define a syslog host in the **System Config -> Network Settings** screen.



Email History

Every message that passes through the 3Com Email Firewall generates a database entry that records information about how it was processed, including a detailed journal identifying the results of the mail processing.

Select **Reporting -> Email History** from the menu to view the message history.

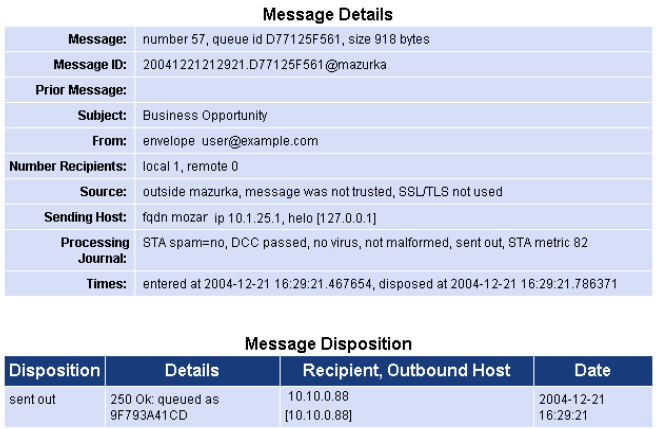


Message List
Records 1 to 30 (of 150)

Search: queue ID for: Match Case: Search Help

Queue ID	Time Received	Subject	Prior	Journal
F16AE33B8E	2005-01-13 13:21:53.002856	Report rep6.html from w81: Full Report		sent out
F2DC28A063	2005-01-13 13:15:25.15904	Undelivered Mail Returned to Sender	0B1F6DA64E	deferred
4BB7D68DB5	2005-01-13 13:15:21.366724	Undelivered Mail Returned to Sender	3D28FDE93E	deferred
B142108230	2005-01-13 13:15:21.009054	Undelivered Mail Returned to Sender	7569103ECB	deferred
F4F10E277E	2005-01-13 13:15:19.197071	Undelivered Mail Returned to Sender	22153738F7	deferred
C23C49EC31	2005-01-13 13:15:19.185125	Undelivered Mail Returned to Sender	0D6B7B156C	deferred
91992289EF	2005-01-13 13:15:16.150225	Undelivered Mail Returned to Sender	1A7C1A6AF0	deferred
A926173E60	2005-01-13 13:15:15.579288	Undelivered Mail Returned to Sender	D6D274CF40	deferred

You can quickly search the email history by entering a specific field to search on and a pattern. Click on an individual message **Queue ID** to display the details for the message and how it was processed.



Message Details

Message:	number 57, queue id D77125F561, size 918 bytes
Message ID:	20041221212921.D77125F561@mazurka
Prior Message:	
Subject:	Business Opportunity
From:	envelope user@example.com
Number Recipients:	local 1, remote 0
Source:	outside mazurka, message was not trusted, SSL/TLS not used
Sending Host:	fqdn mozar ip 10.1.25.1, helo [127.0.0.1]
Processing Journal:	STA spam=no, DCC passed, no virus, not malformed, sent out, STA metric 82
Times:	entered at 2004-12-21 16:29:21.467654, disposed at 2004-12-21 16:29:21.786371

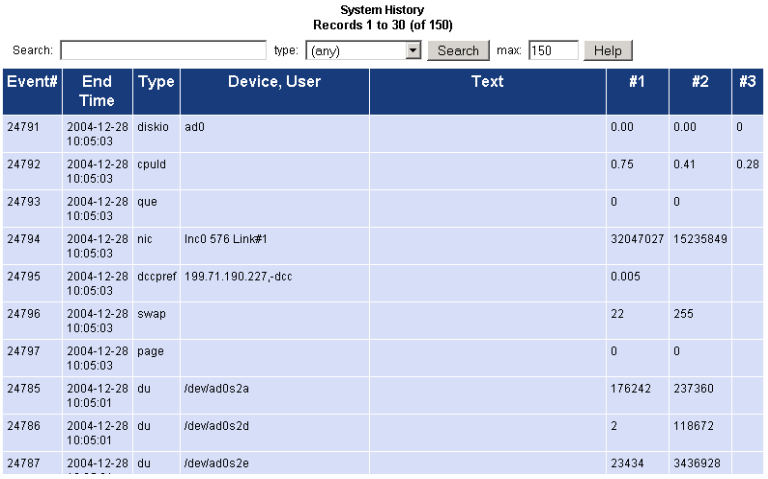
Message Disposition

Disposition	Details	Recipient, Outbound Host	Date
sent out	250 Ok: queued as 9F793A41CD	10.10.0.88 [10.10.0.88]	2004-12-21 16:29:21

System History

The system history is a record of system events, such as login failures, and disk space and CPU usage.

Select **Reporting -> System History** from the menu to view the system event history.



System History
Records 1 to 30 (of 150)

Search: type: (any) Search max: 150 Help

Event#	End Time	Type	Device, User	Text	#1	#2	#3
24791	2004-12-28 10:05:03	diskio	ad0		0.00	0.00	0
24792	2004-12-28 10:05:03	cpuld			0.75	0.41	0.28
24793	2004-12-28 10:05:03	que			0	0	
24794	2004-12-28 10:05:03	nic	Inc0 576 Link#1		32047027	15235849	
24795	2004-12-28 10:05:03	dccpref	199.71.190.227,-dcc		0.005		
24796	2004-12-28 10:05:03	swap			22	255	
24797	2004-12-28 10:05:03	page			0	0	
24785	2004-12-28 10:05:01	du	/dev/ad0s2a		176242	237360	
24786	2004-12-28 10:05:01	du	/dev/ad0s2d		2	118672	
24787	2004-12-28	du	/dev/ad0s2e		23434	3436928	

Event Types

The following table describes the event types that can appear in the System History database.

Table 4 System Events

Event Type	Description	Parameters
Admin Actions	Shows administrative functions that have been performed	
AV Updates	The time of the last update, its success or failure, and the name of the new pattern file	
CPU Load	The load average for the past 1, 5, and 15 minutes	Number of processes waiting for CPU. A very busy system may have 50 or more.

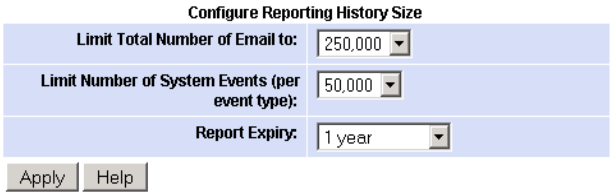
Event Type	Description	Parameters
DCC Preferred	The round trip time to preferred DCC server	Name of preferred server
Disk IO	MB per second transfer, KB per transfer, transfers per second for a disk	
Disk Usage	Amount of used and total available disk space for each disk slice	
Logins	A single web based login	UserID and IP address
Logouts	A single web based logout (not including timed-out sessions)	UserID and IP address
Login failure	Login failure	UserID and IP address
Network IO	Amount of data in and out of network card	
Paging	This shows the swap paging activity (pages in/out) over 5 seconds	
Queue Sizes	Number of messages in active and deferred queues	Active queue size in bytes, deferred queue size in bytes
RBL Responses	Average round time to RBL server with minimum and maximum values	RBL server
Swap usage	This shows the swap usage, and total swap space available	Used and available swap space in megabytes

Configure History Settings

In the *Configure Reporting History Size* screen, you can configure how many emails and system events to keep in the logs and how long you want to keep them.

Setting higher values will use up more disk space and cause backups to take much longer to complete if they include the reporting data.

Select **Reporting -> Configure History** from the menu to modify your reporting history settings.



- Limit Total Number of Email to — Select the total number of emails to keep in the email history.
- Limit Number of System Events (per event type) — Select the limit for the number of system events to keep.
- Report Expiry — Choose how long you wish to keep reports.

6 SYSTEM CONFIGURATION

This chapter describes how to view and modify the system configuration of the 3Com Email Firewall, and includes the following topics:

- Setup Wizard
- Admin Account
- System Users
- Network Settings
- Web Proxy
- Static Routes
- Licensing
- SSL Certificates
- Software Updates

Setup Wizard

The Setup Wizard can quickly guide you through the steps to change your networking or system mail setup information. For additional information regarding the Setup Wizard, refer to the *Installation Guide* that you received with your 3Com Email Firewall.

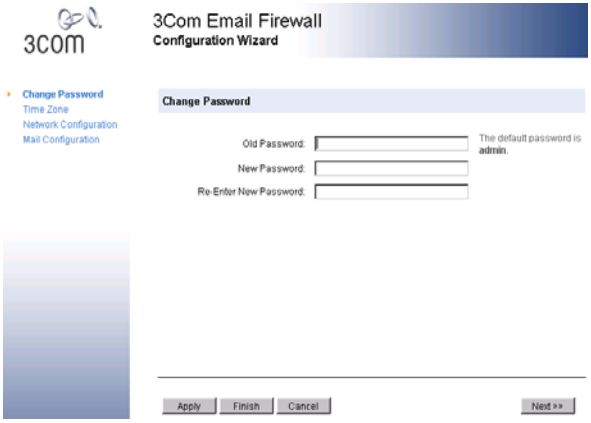
Using the Setup Wizard, you can change the following settings:

- Admin Password
- Time Zone
- Network Configuration
- Mail Configuration

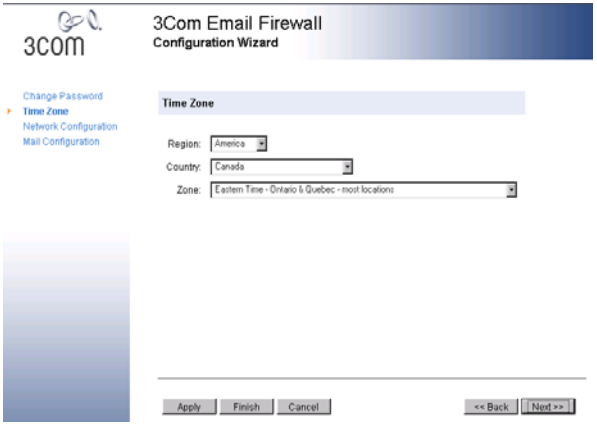
Select **System Config -> Setup Wizard** from the menu to start the Setup Wizard.

*Click Finish at any time to exit the Setup Wizard. Click **Back** to go to the previous step.*

Change Password Enter your old password and set a new password if required. Click **Apply** if you have made any changes. If you do not want to modify your current password, leave all fields blank and click **Next** to continue.

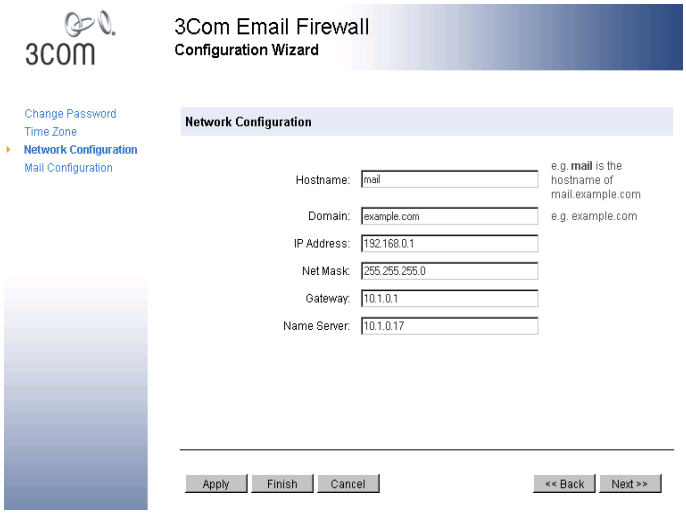


Time Zone Modify your time zone, if required. Click **Apply** if you have made any changes. If you do not want to modify your time zone information, click **Next** to continue.



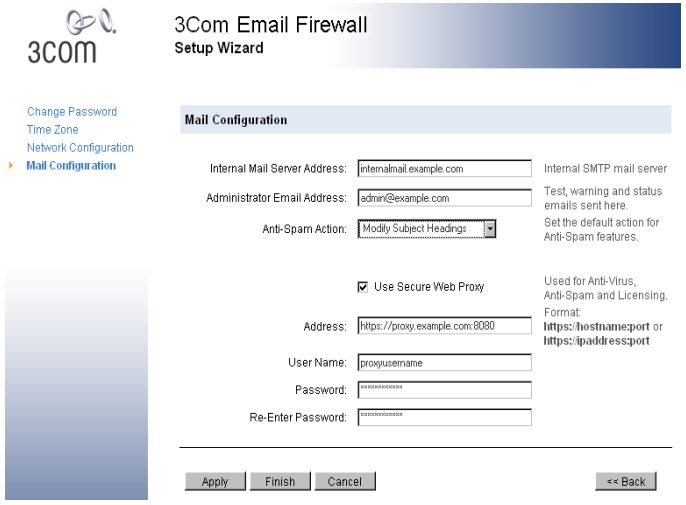
Network Configuration

Modify your network settings if required, and click **Apply** if you have made any changes. If you do not want to modify your networking information, click **Next** to continue.



Mail Configuration

Modify your mail configuration and proxy settings if required, and click **Apply** if you have made any changes. If you do not want to modify your mail configuration settings, click **Finish**.



Admin Account

Select **System Config -> Admin Account** from the menu to modify the administrator account settings.

You can modify the address to which mail to the administrator is forwarded to, and change the admin account password.

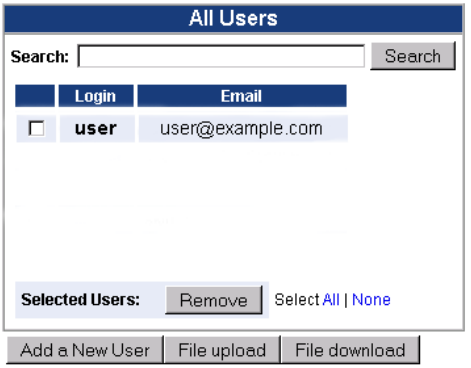
CAUTION: If you forget your admin password, you will have to reinstall the system. Please choose your password carefully, and store it in a safe place. See Appendix B on page 127 for information on resetting the system if you have forgotten your admin password.

Click **Add Admin User** to create a new user with admin privileges.

System Users

You must add local users to the 3Com Email Firewall if you require the ability to view the user Spam Quarantine or configure the Trusted Senders Lists.

Select **System Config -> Users** to manage your local users.



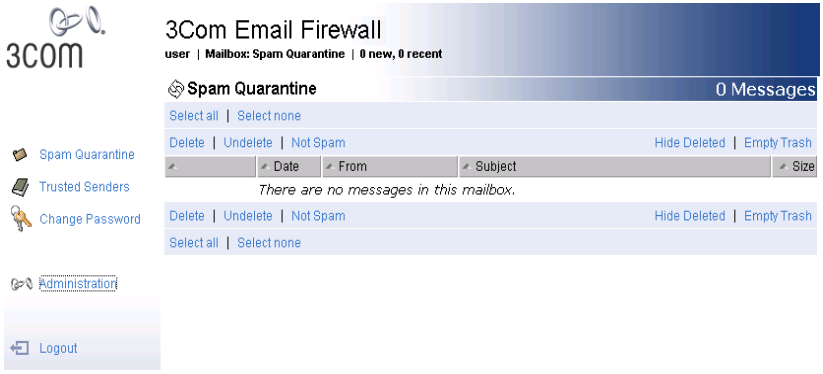
Click the **Add a New User button** to add a new user to the system.

Enter a User ID and a Password.

Creating an Admin User

If this user will be an additional administrator for this 3Com Email Firewall, select the **Full Admin** option in the *Administrator Privileges* section.

When a **Full Admin** user logs into the 3Com Email Firewall, they must click the **Administration** link on the left menu to open up the admin menu.



Upload and Download User Lists

You can upload lists of users using comma or tab separated text files. You can specify the login ID, password, email address, and disk quota in megabytes. Use the following format:

[login],[password],[email address],[quota]

For example,

user,ajg7rY,user@example.com,0

The file (*user.csv*) should be created in csv file format using Excel, Notepad or other Windows text editor. It is recommended that you download the user list file first by clicking **File Download**, editing it as required, and then uploading it using the **File Upload** button.

Enabling User Access on a Network Interface

You must enable User Access on the network interface to allow users to log in via that interface.

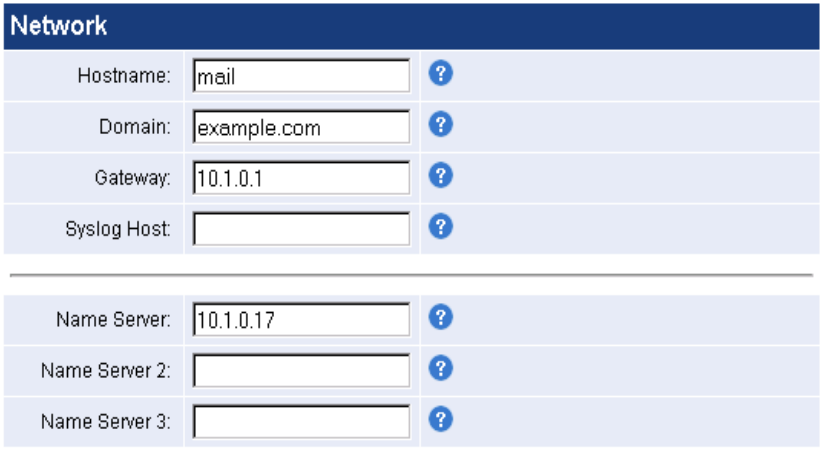
Select **System Config -> Network Settings** and go to the *Network Interface* section.

Select the **User Access** check box to allow local access to the Spam Quarantine and Trusted Senders List via this interface. Click **Apply** to save the network settings.

Network Settings

The *Network Settings* screen allows you to modify your network settings such as the Hostname, Domain name, IP address, Name Server, and network interface settings.

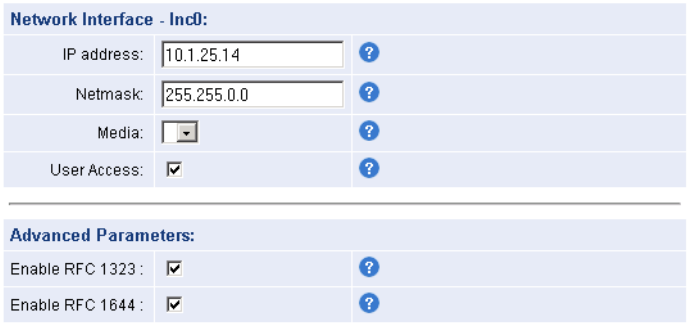
Select **System Config -> Network Settings** from the menu to manage your networking information.



- Hostname — Enter the hostname (not the full domain name) of the 3Com Email Firewall, such as *mail* in the domain name *mail.example.com*.
- Domain — Enter the domain name, such as *example.com*.
- Gateway — Enter the default gateway for this 3Com Email Firewall. This is typically your network router.
- Syslog host — Enter an optional *syslog* host to forward logs to. A *syslog* server collects and stores log files from many sources.
- Name Server — Enter the address of your DNS server, and enter secondary name servers if required.

Network Interfaces

In the *Network Interfaces* section, you can modify your network interface information such as the IP address, netmask, and enable local user access.



- IP Address — Enter the IP address for this 3Com Email Firewall.
- Netmask — Enter the appropriate netmask for your network.
- Media — Select the type of network card. Use *Auto select* for automatic configuration.
- User Access — Enables local access to the Spam Quarantine and Trusted Senders List on this interface.

Advanced Parameters

The following advanced network parameters are enabled by default and should only be modified if you are experiencing connection problems with certain mail delivery hosts.

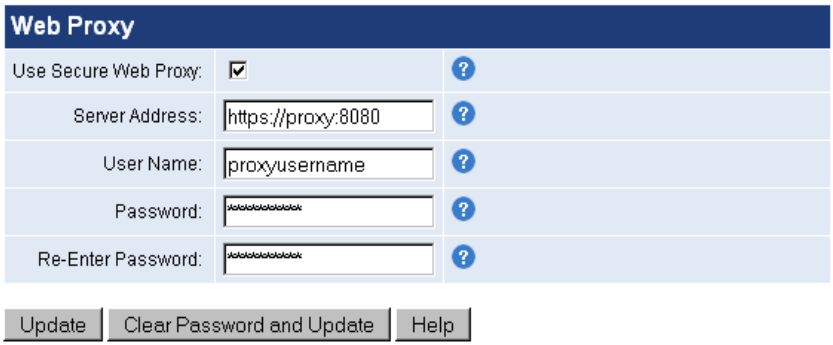
- Enable RFC 1323 — These are TCP extensions to improve performance and to provide reliable operation over very high-speed paths.
- Enable RFC 1644 — This is an experimental TCP extension for efficient transaction-oriented (request/response) service.

Web Proxy

A secure proxy server may be used to cache and proxy requests to systems external to your network, such as an HTTP web proxy server.

If you use a proxy server on your network, you must enter the proxy server address and a username and password to allow Anti-Virus, Anti-Spam, and Licensing services to retrieve updates.

Select **System Config -> Web Proxy** from the menu.

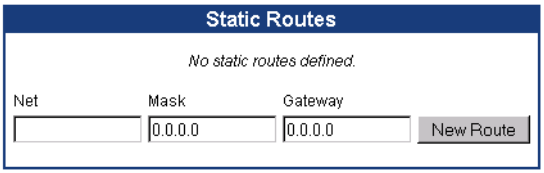


- Use Secure Web Proxy — Select the check box to enable use of the secure web proxy.
- Server Address — Enter the proxy server address in the format https://hostname:port, such as *https://proxy.example.com:8080*.
- User Name — Enter a username to log into the secure web proxy server.
- Password — Enter a corresponding password for the user name you entered.
- Re-Enter Password — Confirm the password.

Static Routes

Static routes are required if the mail servers to which mail must be relayed are located on another network, such as behind an internal firewall or accessed via a VPN.

Select **System Config -> Static Routes** from the menu to define any static routes.

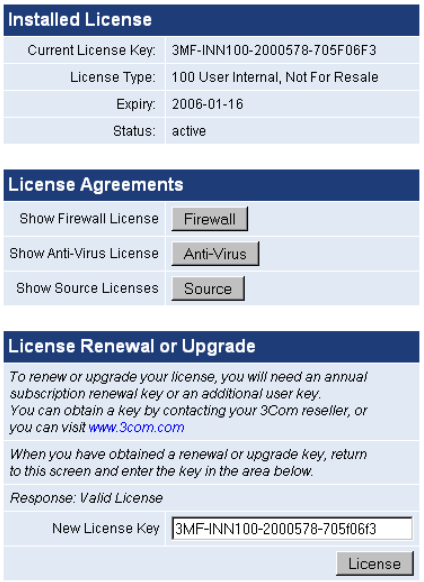


To add a new static route, enter the network address, netmask and gateway for the route, and then click **New Route**.

Licensing

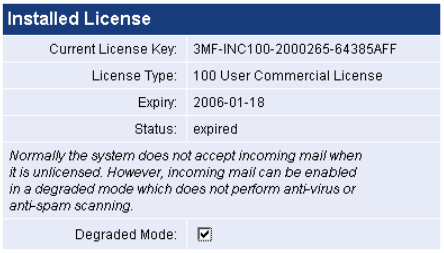
Your 3Com Email Firewall must be licensed before it can process mail. The *Licensing* screen allows you to view your current license information and enter a new license key if you are renewing or upgrading your current license.

Select **System Config -> Licensing** from the menu to view and manage your license information.


Installed License
Current License Key: 3MF-INN100-2000578-705F06F3
License Type: 100 User Internal, Not For Resale
Expiry: 2006-01-16
Status: active
License Agreements
Show Firewall License
Firewall
Show Anti-Virus License
Anti-Virus
Show Source Licenses
Source
License Renewal or Upgrade
To renew or upgrade your license, you will need an annual subscription renewal key or an additional user key.
You can obtain a key by contacting your 3Com reseller, or you can visit www.3com.com
When you have obtained a renewal or upgrade key, return to this screen and enter the key in the area below.
Response: Valid License
New License Key
3MF-INN100-2000578-705f06f3
License

Installed License

The *Installed License* section displays your current license information. If your license expires, the system will not accept incoming mail connections. You can switch to *Degraded* mode by selecting the corresponding check box which will allow you to accept mail, but the Anti-Spam and Anti-Virus services will not scan these messages.


Installed License
Current License Key: 3MF-INC100-2000265-64385AFF
License Type: 100 User Commercial License
Expiry: 2006-01-18
Status: expired
Normally the system does not accept incoming mail when it is unlicensed. However, incoming mail can be enabled in a degraded mode which does not perform anti-virus or anti-spam scanning.
Degraded Mode:

License Agreements

Click the specified button to view the license agreements for the 3Com Email Firewall, the Anti-Virus software, and Third Party Open Source products.

License Renewal or Upgrade

To renew or upgrade your license, you will need an annual subscription renewal key or an additional user key. You can obtain a key by contacting your 3Com reseller, or you can visit *www.3com.com.*

When you have obtained a renewal or upgrade key, return to this screen and enter the key in the *New License Key* field and click **License**.

SSL Certificates

A valid SSL certificate is required to support the encryption services available on the 3Com Email Firewall. The SSL encrypted channel from the server to the web browser (such as when using a URL that begins with *https*), requires a valid digital certificate. You can use self-signed certificates generated by the 3Com Email Firewall, or import certificates purchased from commercial Certificate Authorities (CA) such as Verisign.

The disadvantage of self-signed certificates is that web browsers will display warnings that the "company" (in this case, the 3Com Email Firewall) issuing the certificate is untrusted. When you purchase a commercial certificate, the browser will recognize the company that signed the certificate and will not generate the warning messages.

A web server digital certificate can only contain one domain name, such as *server.example.com*, and a limitation in the SSL protocol only allows one certificate per IP address. Some web browsers will display a warning message when trying to connect to any domain on the server that has a different domain name than the server specified in the single certificate. Digital certificates eventually expire and are no longer valid after a certain period of time, and need to be renewed before the expiry date.

To install a commercial certificate:

1 Select **System Config -> SSL Certificates** from the menu to view and manage your certificates.

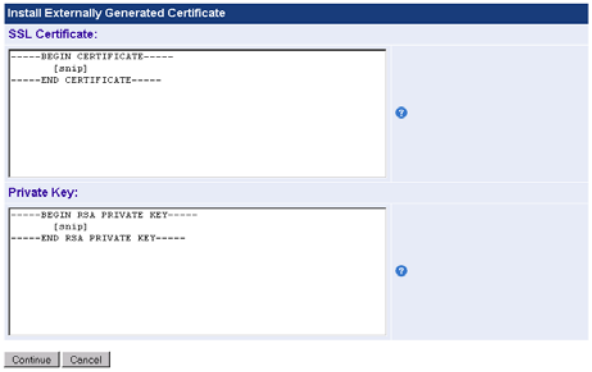
2 Create a new self-signed certificate by clicking the **Generate a 'self-signed' certificate** button.

3 Click **Apply**. You must then reboot to install the new certificate.

4 Click the **Show installed certificate button** to display the certificate and an accompanying certificate request.

5 Forward the request portion of the certificate to a commercial Certificate Authority (CA) for signing.

6 When received, install the commercial certificate by clicking the **Load a site certificate** button. Copy and paste the SSL Certificate and private key portions into the indicated fields, and then click **Continue**.



7 When completed, click **Show installed certificate** to ensure the certificate is loaded and that the information is correct.

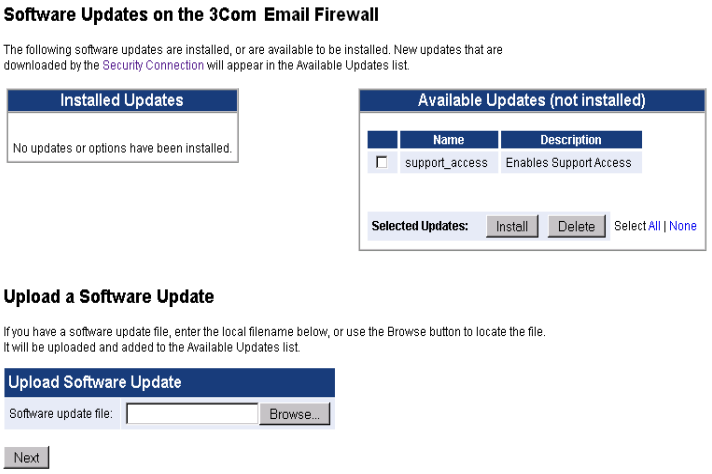
Software Updates

It is important to keep your 3Com Email Firewall software updated with the latest patches and upgrades. A key aspect of good security is responding quickly to new attacks and exposures by updating the system software when updates are available.

Software updates can be delivered or retrieved using a variety of methods, including email, FTP, or from 3Com's support servers. The *Security Connection*, if enabled, will download any patches automatically and notify you when they are available.

The *Update Software* screen shows updates that are *Available Updates* (loaded onto the 3Com Email Firewall, but not applied) and *Installed Updates* (applied and active.) You can install an available update, or uninstall a previously installed update.

Select **System Config -> Software Updates** from the menu to install new updates.


Software Updates on the 3Com Email Firewall
The following software updates are installed, or are available to be installed. New updates that are downloaded by the Security Connection will appear in the Available Updates list.
Installed Updates
No updates or options have been installed.
Available Updates (not installed)
Name
Description
support_access
Enables Support Access
Selected Updates:
Install
Delete
Select All | None
Upload a Software Update
If you have a software update file, enter the local filename below, or use the Browse button to locate the file. It will be uploaded and added to the Available Updates list.
Upload Software Update
Software update file:
Browse...
Next

Uploading a Software Update

When these software update files are downloaded to your local system, they can be installed by clicking **Browse** in the *Upload a Software Update* section, navigating to the downloaded file, and then clicking **Next**.

The update will now appear in the *Available Updates (not installed)* section. Click on the update you want to apply, then click **Install**. After applying any updates, you must restart the system.

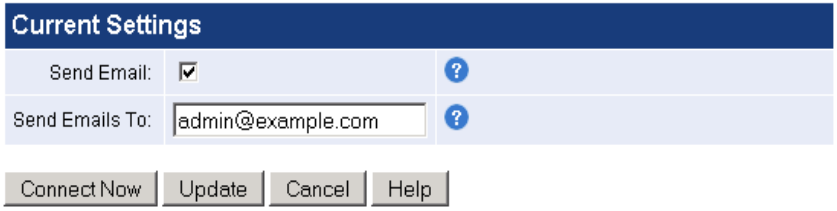
When the system restarts, the update will appear in the *Installed Updates* section.

Before applying any update, backup your system configuration and data. Select ***System Mgmt -> Backup & Restore*** *from the menu to perform a backup.*

Security Connection

The *Security Connection* is a service running on the 3Com Email Firewall that polls 3Com's support servers for new updates, security alerts, and other important information. When new information and updates are received, an email can be sent to the administrator.

Click the **Security Connection** link in the **System Config -> Software Updates** screen.



- Send Email — Enable this option to send an email to the address specified in the *Send Emails To* field when an Email Firewall update is available.
- Send Emails To — Specify an email address to receive messages from Security Connection.

Click the **Connect Now** button to run Security Connection immediately.

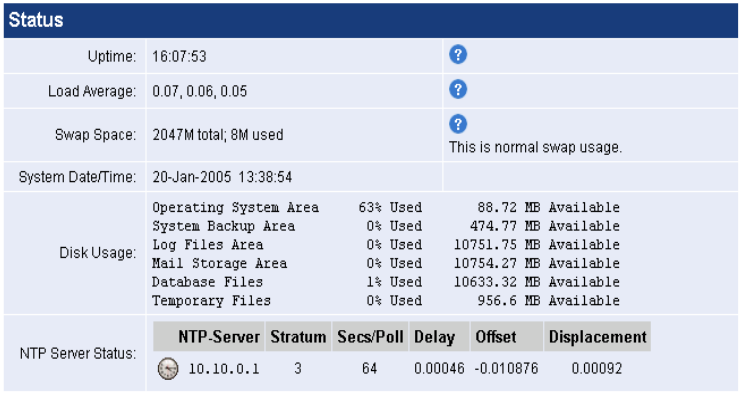
7 SYSTEM MANAGEMENT

This chapter describes how to use the system management features of the 3Com Email Firewall, and includes the following topics:

- Status and Utility
- Mail Queues
- Quarantine
- Daily Tasks
- Backup and Restore
- Reboot and Shutdown
- Reset to Factory Settings

Status and Utility

Select **System Mgmt -> Status and Utility** from the menu to view a number of system statistics such as the total system uptime, load average, the amount of used swap and disk partition space, and NTP server status.



Status

Uptime:	16:07:53	
Load Average:	0.07, 0.06, 0.05	
Swap Space:	2047M total; 8M used	This is normal swap usage.
System Date/Time:	20-Jan-2005 13:38:54	

Disk Usage:

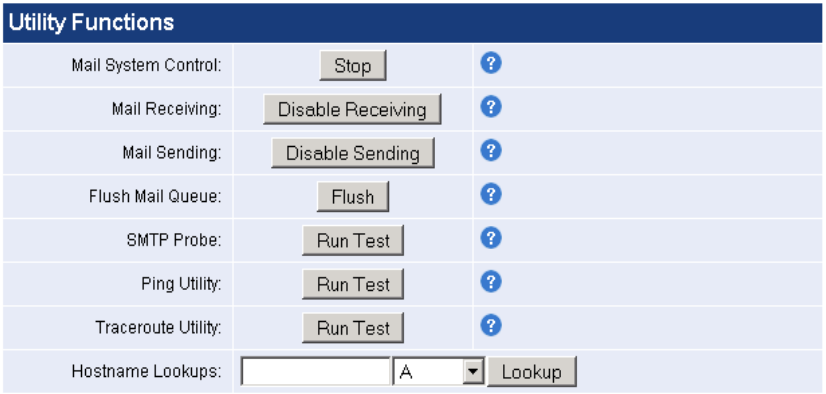
Operating System Area	63% Used	88.72 MB Available
System Backup Area	0% Used	474.77 MB Available
Log Files Area	0% Used	10751.75 MB Available
Mail Storage Area	0% Used	10754.27 MB Available
Database Files	1% Used	10633.32 MB Available
Temporary Files	0% Used	956.6 MB Available

NTP Server Status:

NTP-Server	Stratum	Secs/Poll	Delay	Offset	Displacement
10.10.0.1	3	64	0.00046	-0.010876	0.00092

Utility Functions

The *Utility Functions* section allows you to control mail services and run network and diagnostic utilities.



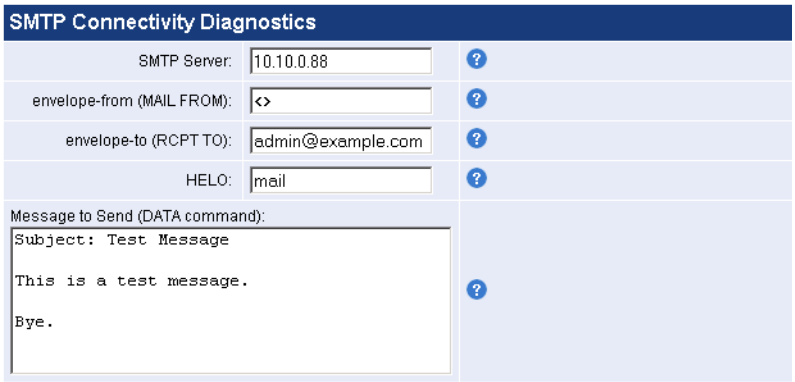
- Mail System Control — Use this button to Stop and Start all mail queues.
- Mail Receiving — Use this button to disable and enable mail receiving only.
- Mail Sending — Use this button to disable and enable mail sending only.
- Flush Mail Queue — The **Flush Mail Queue** button is used reprocess any queued mail in the system. Only click this button once. If the mail queue does not process, you may be experiencing other types of delivery problems and reprocessing the mail queue will only add additional load to the system.

SMTP Probe

The SMTP (Simple Mail Transport Protocol) Probe is used to test email connectivity with a remote SMTP server. This allows you to verify that a specific SMTP server is responding to connection requests and returning a valid response.

In the SMTP Probe screen you must enter the destination SMTP server, the envelope header fields for the sender and recipient (MAIL FROM and RCPT TO), the HELO identifier, and the message data.

Click the **Send Message** button to send the test message to the destination SMTP server. The server should come back with a response.



- SMTP Server — Enter the domain name of the destination SMTP server that you want to test.
- Envelope-from (MAIL FROM) — The MAIL FROM part of the email message identifies the sender. Enter an email address indicating the sender of the message.
- Envelope-to (RCPT TO) — The RCPT TO part of the email message identifies the recipient of the email. Enter an email address indicating the intended recipient of the message.
- HELO — The HELO parameter is used to identify the SMTP Client to the SMTP Server. You can enter any value here, but the sending domain name of the server is usually specified.
- Message to Send (DATA Command) — This contains the actual test message data. You can enter an optional subject to ensure a blank subject field is not sent.

The response field will show the result of the SMTP diagnostic probe, including the response for each SMTP command sent:

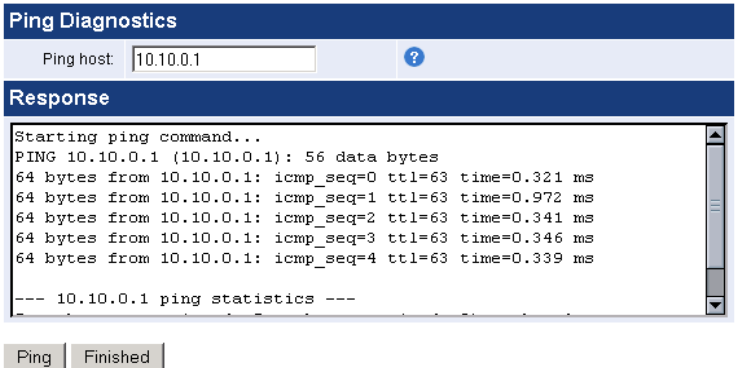
```
Sending mail...
<<< 220 ESMTP Postfix (2.1.0)
HELO example.com
<<< 250 mail.example.com
MAIL FROM:sender@example.com
<<< 250 Ok
RCPT TO:joe@example.com
<<< 250 Ok
DATA
<<< 354 End data with <CR><LF>.<CR><LF>
sending /tmp/smtpdata
<<< 250 Ok: queued as F130F33EA6
QUIT
<<< 221 Bye
```

Ping Utility

The ping utility sends ICMP packets to a host and listens for a return packet. This ensures that you have network connectivity to the destination server. If you do not receive a response, the destination host may not be available or it may indicate that your 3Com Email Firewall does not have network connectivity.

Try to ping other hosts internal and external to your network. If you cannot ping any hosts external to your network, your Internet connection is most likely down.

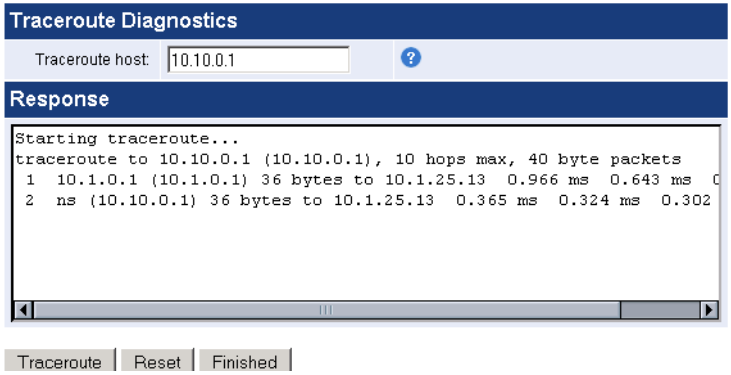
For more detailed information on routing connectivity between the two hosts, use the **traceroute** utility.


Ping Diagnostics
Ping host:
10.10.0.1
Response
Starting ping command...
PING 10.10.0.1 (10.10.0.1): 56 data bytes
64 bytes from 10.10.0.1: icmp_seq=0 ttl=63 time=0.321 ms
64 bytes from 10.10.0.1: icmp_seq=1 ttl=63 time=0.972 ms
64 bytes from 10.10.0.1: icmp_seq=2 ttl=63 time=0.341 ms
64 bytes from 10.10.0.1: icmp_seq=3 ttl=63 time=0.346 ms
64 bytes from 10.10.0.1: icmp_seq=4 ttl=63 time=0.339 ms
--- 10.10.0.1 ping statistics ---
Ping
Finished

Traceroute Utility

Traceroute is used to see the routing steps between two hosts. If you are losing connectivity somewhere in between the two hosts, you can use traceroute to see where exactly the packet is losing its connection.

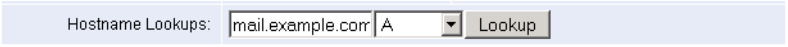
The traceroute utility will show each network "hop" as it passes through each router to its destination. If you are experiencing routing issues, you will be able to see in the trace response where exactly the communication is failing.


Traceroute Diagnostics
Traceroute host:
10.10.0.1
Response
Starting traceroute...
traceroute to 10.10.0.1 (10.10.0.1), 10 hops max, 40 byte packets
1 10.1.0.1 (10.1.0.1) 36 bytes to 10.1.25.13 0.966 ms 0.643 ms
2 ns (10.10.0.1) 36 bytes to 10.1.25.13 0.365 ms 0.324 ms 0.302
Traceroute
Reset
Finished

Hostname Lookups

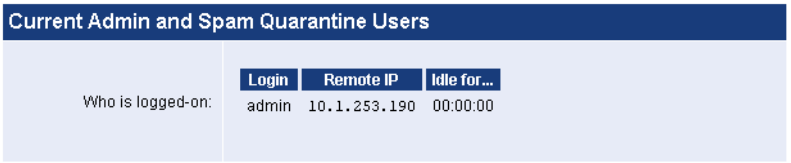
Use the hostname lookup utility to ensure your DNS services are working properly. Enter a hostname and the type of record you are looking up (such as an "A" record.)

Click **Lookup** to query the DNS server with the specified host.



Current Admin and Spam Quarantine Users

The *Current Admin and Spam Quarantine Users* section displays who is logged in via the admin interface or through a Spam Quarantine session.



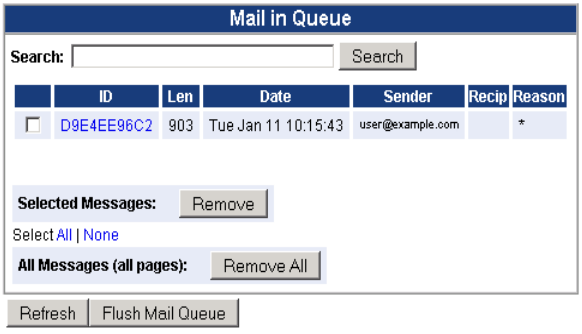
Configuration Information

The configuration information screen shows you important system information such as the current version of the system software, the time it was installed, and CPU and RAM information.

Mail Queues

Select **System Mgmt -> Mail Queues** to view and manage queued mail.

The *Mail Queues* screen contains information on mail waiting to be delivered. You can search for a specific mail message using the search function. Messages that appear to be undeliverable can be removed by selecting them and then clicking the **Remove** button.



Quarantine

The *Quarantine* area contains messages that have been quarantined because of a virus, malformed message, illegal attachment, or other issue.

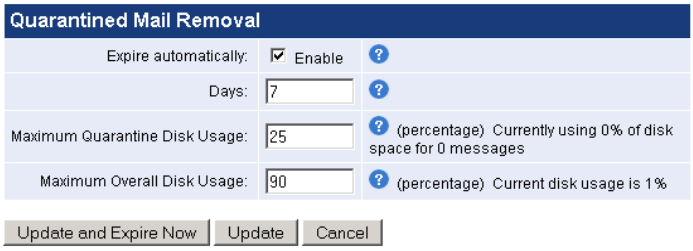
Select **System Mgmt -> Quarantine** to view and manage the quarantine area.

You can view the details of a message by clicking on its ID number or remove the message from quarantine by clicking the **Remove** button. Quarantined messages can also be forwarded to their original destination by clicking the **Forward to Original Recipient** button.

Use the search field to look for specific messages within the quarantine. For example, you could search for the name of a specific virus so that any quarantined messages infected with that virus will be displayed.

Expiry Settings

Click the **Set Expiry Settings** button to configure the quarantine expiry settings. An expiry term can be set so that messages will be deleted after a certain period of time. You can use this feature to flush all messages from the quarantine area on a regular basis.



- Expire automatically — Enable this feature to expire messages automatically.
- Days — Enter how many days to keep a quarantined message before deleting it.
- Maximum Quarantine Disk Usage (percentage) — Enter a percentage of disk usage that can be used by the quarantine area. If the quarantine area grows beyond this size, messages will be expired.
- Maximum Overall Disk Usage (percentage) — Enter a percentage for the maximum overall disk usage that can be used by the quarantine.

Click **Update** to enable the settings for new quarantined messages. Click **Update and Expire Now** to apply the settings to all messages in the quarantine area.

Daily Tasks

The *Daily Tasks* feature allows you to set up daily recurring FTP and Email backups.

The FTP backup and Email backup features must be configured separately in the **System Mgmt -> Backup & Restore** screen for the daily tasks to work.

Select **System Mgmt -> Daily Tasks** to configure recurring backups.

- FTP Backup — Enables recurring FTP backups.
- Email Backup — Enables recurring Email backups.
- Start Time — Set the start time using the 24 hour format *hh:mm*.

Backup and Restore

The 3Com Email Firewall can backup all data, including the database, quarantined items, mail queues, mailboxes, uploaded user lists, SSL certificates, reports, and system configuration data. The restore feature can restore any of these items individually. The 3Com Email Firewall should be backed up before performing any type of software upgrade or update.

Starting a Backup

You can perform backups on demand, or you can schedule a tape or FTP backup once per day via the *Daily Tasks* option from the **System Mgmt -> Daily Tasks** screen.

The Email Firewall supports three backup methods:

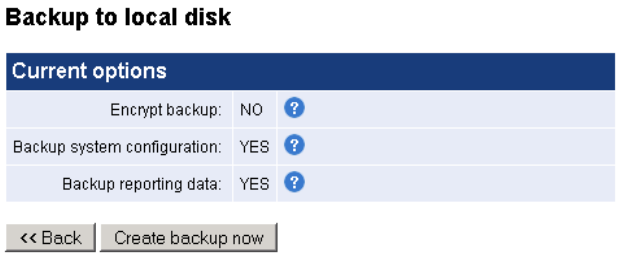
- FTP server
- Local Disk
- Email to admin (Configuration only)

Select the type of backup and click the **Next >>** button.

Local Disk Options

When backing up to a file on a local disk, you can choose to encrypt the file if required. Click **Next >>** to continue.

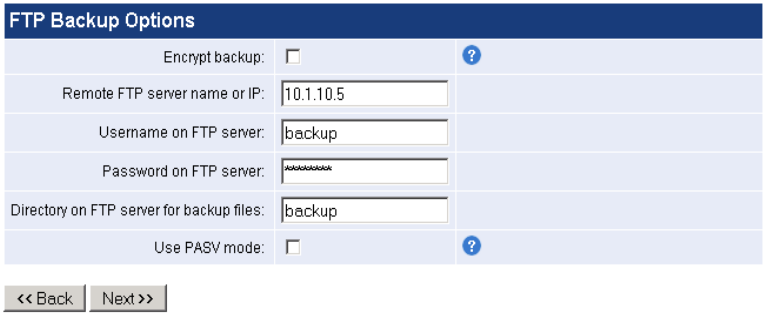
Confirm the listed options, and then click **Create backup now** to begin.



The file (*backup.gz)* will be then be downloaded to your local system.

FTP Options

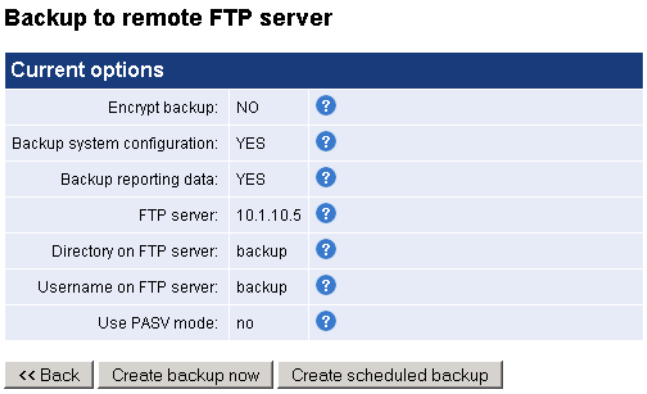
If you choose the FTP option you must specify the address of the destination FTP server, including a valid login and password.


FTP Backup Options
Encrypt backup:
Remote FTP server name or IP: 10.1.10.5
Username on FTP server: backup
Password on FTP server:
Directory on FTP server for backup files: backup
Use PASV mode:
<< Back
Next >>

- Encrypt backup — Select this option to encrypt the backup file.
- Remote FTP server name or IP — Enter the hostname or IP address of the destination FTP server.
- Username on FTP server — Enter the username to log in to this FTP server.
- Password on FTP server — Enter a corresponding password for the username entered.
- Directory on FTP server for backup files — Enter the destination directory on the FTP server to store your backup files.

- Use PASV mode — PASV (Passive) mode may be required for some types of FTP servers. Choose this option if you are having problems with connecting to your FTP server.

Click **Next >>** to continue.



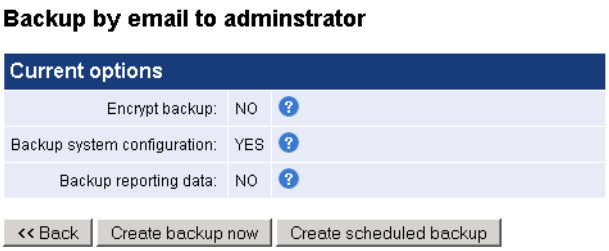
Confirm the listed options, and then click **Create backup now** to begin. Alternately, you can click **Create scheduled backup** to go to the *Daily Tasks* menu to create a recurring FTP backup.

Administrator Backup Email Options

If you select the Email backup type, the configuration will be saved and sent via email attachment to the 3Com Email Firewall administrator. It is recommended that you save the email attachment to your local disk.

System mail and data cannot be backed up using this method. Only the system configuration is saved.

You can choose to encrypt the file if required. Click **Next >>** to continue.



Confirm the listed options, and then click **Create backup now** to begin. Alternately, you can click **Create scheduled backup** to go to the *Daily Tasks* menu to create a recurring Email backup.

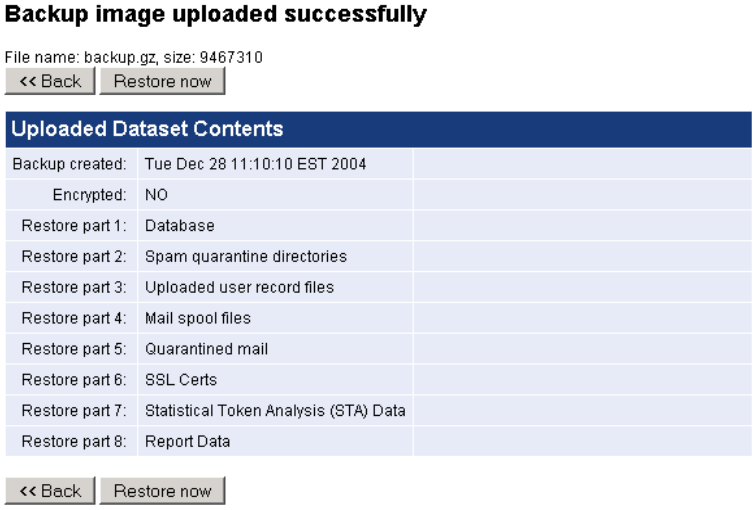
Restores To perform a system restore, select the type of restore to perform (Local Disk or FTP) and click the **Next >>** button.

Restore from Local Disk

To perform a restore from a file on a local disk, click the **Browse** button to find the backup file. If you are restoring from an email backup, you must save the email attachment to the local disk first before performing the restore.

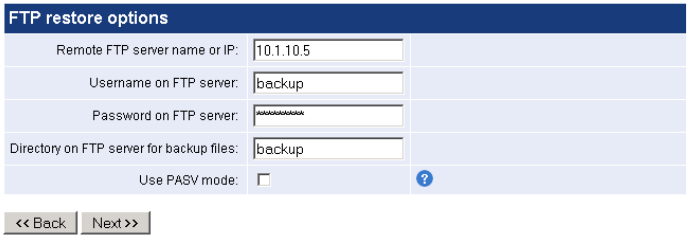
Restore from local disk
Enter the local filename that contains your server's backup data.
Restore 3Com Email Firewall Data
Backup data file:
Browse...
<< Back
Next >>

Click **Next >>** to continue. When the file has been successfully uploaded, confirm the items to restore, and click **Restore now**.


Backup image uploaded successfully
File name: backup.gz, size: 9467310
<< Back
Restore now
Uploaded Dataset Contents
Backup created: Tue Dec 28 11:10:10 EST 2004
Encrypted: NO
Restore part 1: Database
Restore part 2: Spam quarantine directories
Restore part 3: Uploaded user record files
Restore part 4: Mail spool files
Restore part 5: Quarantined mail
Restore part 6: SSL Certs
Restore part 7: Statistical Token Analysis (STA) Data
Restore part 8: Report Data
<< Back
Restore now

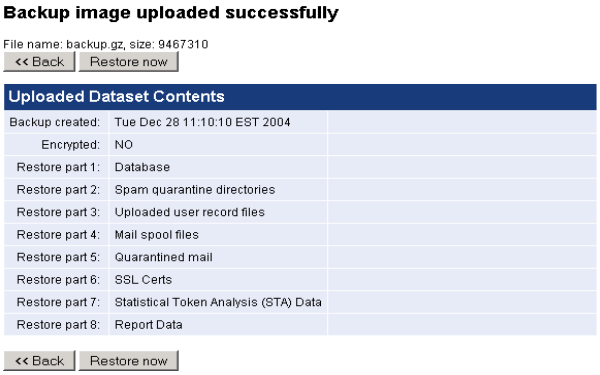
Restore from FTP

To restore from FTP, enter the following required information to connect to your FTP server.



- Remote FTP server name or IP — Enter the hostname or IP address of the destination FTP server.
- Username on FTP server — Enter the username to log in to this FTP server.
- Password on FTP server — Enter a corresponding password for the username entered.
- Directory on FTP server for backup files — Enter the destination directory on the FTP server to store your backup files.
- Use PASV mode — PASV (Passive) mode may be required for some types of FTP servers. Choose this option if you are having problems with connecting to your FTP server.

Click **Next >>** to continue. Confirm the contents of the uploaded file, and then click **Restore now** to perform the restore.


Backup image uploaded successfully
File name: backup.gz, size: 9467310
<< Back
Restore now
Uploaded Dataset Contents
Backup created: Tue Dec 28 11:10:10 EST 2004
Encrypted: NO
Restore part 1: Database
Restore part 2: Spam quarantine directories
Restore part 3: Uploaded user record files
Restore part 4: Mail spool files
Restore part 5: Quarantined mail
Restore part 6: SSL Certs
Restore part 7: Statistical Token Analysis (STA) Data
Restore part 8: Report Data
<< Back
Restore now

Reboot and Shutdown

The 3Com Email Firewall can be safely rebooted or shut down from the **System Mgmt -> Reboot and Shutdown** screen. Before shutting down, remove any media from the floppy and CDROM drives.

3Com Email Firewall Reboot or Shutdown
The 3Com Email Firewall will now be rebooted or shut down.
Reboot now
Shutdown now

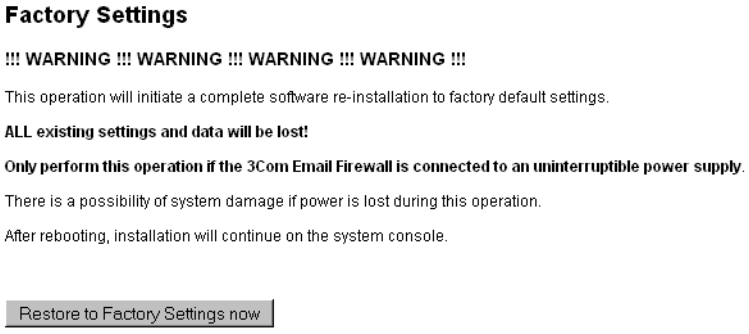
Click **Reboot now** to shutdown the system and reboot.

Click **Shutdown now** to shutdown the system completely.

Reset to Factory Settings

Select **System Mgmt -> Reset to Factory Settings** from the menu to revert your 3Com Email Firewall back to its factory default settings.

CAUTION: *All existing configuration settings and data will be lost if you reset to factory default settings. Ensure that you perform a backup of your system if you wish to restore your configuration and data. Also ensure that your system is connected to a UPS (Uninterruptable Power Supply) to prevent damage in the event of a power failure duing this procedure.*


Factory Settings
!!! WARNING !!! WARNING !!! WARNING !!! WARNING !!!
This operation will initiate a complete software re-installation to factory default settings.
ALL existing settings and data will be lost!
Only perform this operation if the 3Com Email Firewall is connected to an uninterruptible power supply.
There is a possibility of system damage if power is lost during this operation.
After rebooting, installation will continue on the system console.
Restore to Factory Settings now

Click the **Restore to Factory Settings now** button to continue. The system must be rebooted when the procedure is complete. After rebooting, you must reinstall the system using the instructions in the *Installation Guide* that came with your 3Com Email Firewall.

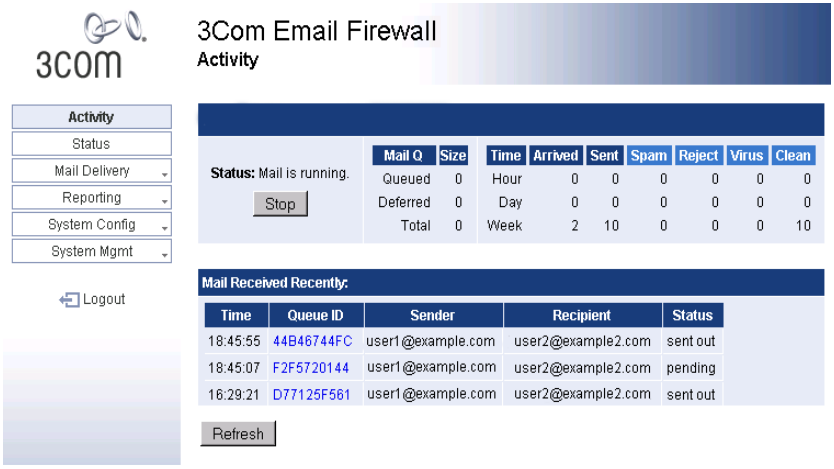
8 MONITORING ACTIVITY AND STATUS

This chapter describes how to monitor the 3Com Email Firewall's mail processing activity and system status, and includes the following topics:

- Monitoring Mail Processing Activity
- Email Firewall Status

Monitoring Mail Processing Activity

Select **Activity** from the main menu to view the 3Com Email Firewall's *Activity* screen. The *Activity* screen provides you with a variety of information on mail processing activity, such as the number of messages in the mail queue, the number of different types of messages received and sent, and current message activity.



Mail Server Status

The mail system status is shown in the top left window. Mail will either be running or stopped. Use the **Stop** or **Start** button to control mail processing.

Mail Queue (Mail Q)

The mail queue activity (Mail Q) section displays the number of *Queued*, *Deferred*, and *Total* messages in the mail queue. This provides a quick indicator of how your mail is processing. If the mail queues begin to build up, you may have a problem sending or accepting mail.

Mail Queue Statistics

The mail queue statistics section displays the number of messages per hour, day and week in the following categories:

- Arrived — The number of messages received.
- Sent — The number of mail messages sent.
- Spam — The number of spam messages received.
- Reject — The number of messages rejected.
- Virus — The number of messages that contained a virus.
- Clean — The number of clean messages that have passed through the system.

Mail Received Recently

The *Mail Received Recently* portion of the *Activity* screen displays the most recent messages processed by the system including their current status. You can click on an individual message ID to see its details.

Troubleshooting Mail Queue Problems

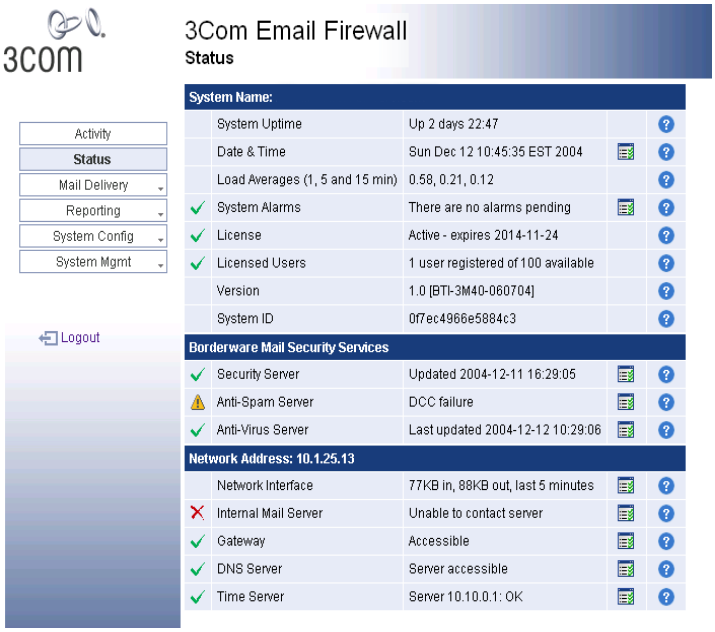
When troubleshooting mail problems, examine the following items on the *Activity* screen:

- Examine the mail queue activity *(Mail Q)* to check the number of *Queued*, *Deferred*, and *Total* messages in the mail queue. This is a quick indicator of how your mail is processing. Click the **Refresh** button frequently to ensure that the mail queues are not building up too high.
- In the *Mail Received Recently* portion of the *Activity* screen, check the timestamps of your most recent incoming and outgoing mail. If no mail has been processed in a certain period of time, this may indicate that the inbound, outbound, or both mail directions are not working.

Check the statistics for your mail queues. You may notice mail system latency if you are receiving a lot of virus, spam, or message rejects.

Email Firewall Status

Select **Status** from the main menu to determine if all services and servers are functioning properly.



For each service, a status icon will indicate if the service is running properly, if there is a warning, or the service is unable to connect.

Ensure that the following services are running and the information displayed is correct.

System Alarms Indicates if there are any pending system alarms. You will receive an alarm if there is an FTP backup error or if a license expires.

Licensing

- License — Displays your license information including the expiration date. If this information is incorrect or if you have installed a license and it does not display as active, please contact 3Com support. A warning icon indicates that your license will expire in a week.
- Licensed Users — Indicates the number of licensed users supported by the 3Com Email Firewall. If this information is incorrect and you have already installed a license, please contact 3Com support. A warning icon indicates that you are using at least 90% of your licensed number of users.

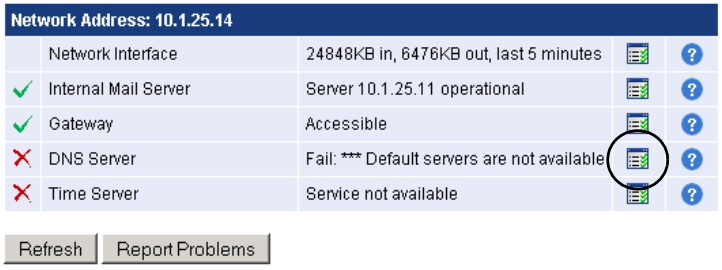
BorderWare Mail Security Services

- Security Server — Indicates the status of the Security Server, and the last time an update was retrieved.
- Anti-Spam Server — Indicates the status of the Anti-Spam server.
- Anti-Virus Server — Indicates the status of your Anti-Virus services, including the time of the last pattern file update.

Network Settings

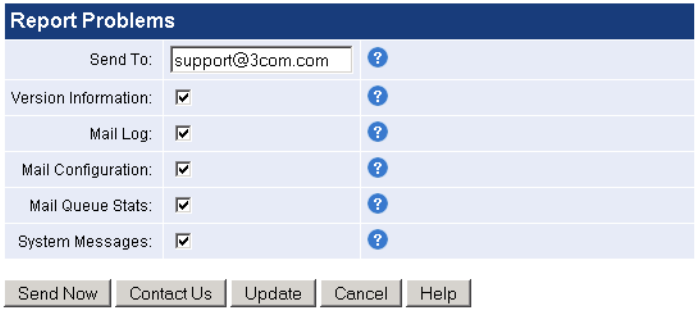
- Internal Mail Server — Indicates the status of your internal mail server. If it is inaccessible, check the internal mail server to ensure that it is running. Perform network tests to ensure you have connectivity between the 3Com Email Firewall and the internal mail server. A warning icon indicates that the connection is timing out.
- Gateway — Indicates your connection to the local gateway, which is your firewall or router. If the gateway is inaccessible, ensure that it is up and running, and perform network tests to ensure connectivity between the 3Com Email Firewall and the gateway.
- DNS Server — Indicates that DNS services are working properly. If the server is inaccessible, check your DNS server to ensure it is running, and perform network tests between the 3Com Email Firewall and the DNS server to ensure they are communicating.
- Time Server — Indicates that your network time server is up and running.

If there are issues with a certain service, click the service check icon beside the help button to perform a test of that particular subsystem.



Report Problems

Click the **Report Problems** button at the bottom of the *Status* page to send selected reports back to 3Com for analysis if you experiencing problems with your 3Com Email Firewall.



- Send to — This is the email address for 3Com support.
- Version information — Include the version information in the problem report.
- Mail Log — Include the Mail Log in the problem report.
- Mail Configuration — Include the Mail Configuration in the problem report.
- Mail Queue Stats — Include the Mail Queue Stats in the problem report.
- System Information — Include the system information in the problem report.

Troubleshooting Mail Delivery Problems

When experiencing any mail delivery problems, the first step is to examine if the problem is affecting only incoming mail, outgoing, or both. For example, if you are receiving mail, but not sending outgoing mail, it is certain that your Internet connection is working properly or you would not be receiving mail. In this scenario, you may have issues with the firewall or router blocking your outbound SMTP connections or some other problem preventing mail delivery.

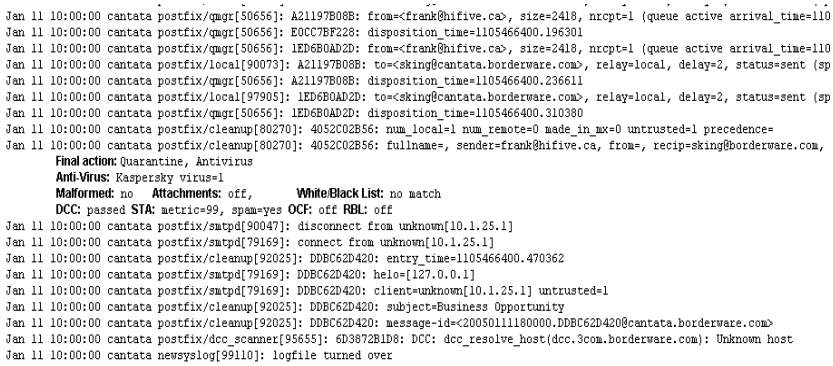
Problems affecting both inbound and outbound delivery include the following scenarios:

- Network infrastructure and Communications — The most common scenario in which you are not receiving or sending mail is if your Internet connection is down. This can include upstream communications with your ISP, your connection to the Internet, or your external router. You should also check your internal network infrastructure to ensure you can contact the 3Com Email Firewall from your router or firewall.
- DNS — If your DNS is not working or configured properly, mail will not be forwarded to your 3Com Email Firewall or you will not be able to lookup external mail sites. Check the DNS service itself to see if it is running and check your DNS records for any misconfiguration for your mail services.
- Firewall/Router — If you are having issues with your firewall or router, or if they have been misconfigured, this may inadvertently block mail access to and from the 3Com Email Firewall. For example, SMTP port 25 must be opened between the Internet and the 3Com Email Firewall to allow inbound and outbound mail connections.
- Internal Mail Systems — You may be receiving incoming mail to the 3Com Email Firewall, but mail is not being forwarded to the appropriate internal mail servers (such as Exchange). Also, outgoing mail from the internal servers may not be forwarded to the 3Com Email Firewall for delivery. In these scenarios, examine your internal mail server to ensure it is working properly. Check communications between the two systems to ensure there are no network, DNS, or routing issues. Also check that your internal servers are configured to send outgoing mail to 3Com Email Firewall.
- External Mail Systems — If you have sent a large amount of mail to a particular destination and that mail server is currently down, these messages will queue up in the deferred mail queue to be retried after

a period of time. You can view the *Mail Transport* logs to see the relevant messages that may indicate why you cannot connect to that particular mail server. The server could be down, too busy, or not currently accepting connections.

Examining Log Files

Examine the system log files in the **Reporting -> System Logs** screen. The **Mail Transport** log is the most important as it provides a detailed description of each message that passes through the system.


Jan 11 10:00:00 cantata postfix/qmgr[50656]: A21197B08B: from=<frank@hifive.ca>, size=2418, nrcpt=1 (queue active arrival_time=110
Jan 11 10:00:00 cantata postfix/qmgr[50656]: E0CC7BF228: disposition_time=1105466400.196301
Jan 11 10:00:00 cantata postfix/qmgr[50656]: 1ED6B0AD2D: from=<frank@hifive.ca>, size=2418, nrcpt=1 (queue active arrival_time=110
Jan 11 10:00:00 cantata postfix/local[90073]: A21197B08B: to=<sking@cantata.borderware.com>, relay=local, delay=2, status=sent (sp
Jan 11 10:00:00 cantata postfix/qmgr[50656]: A21197B08B: disposition_time=1105466400.236611
Jan 11 10:00:00 cantata postfix/local[97905]: 1ED6B0AD2D: to=<sking@cantata.borderware.com>, relay=local, delay=2, status=sent (sp
Jan 11 10:00:00 cantata postfix/qmgr[50656]: 1ED6B0AD2D: disposition_time=1105466400.310380
Jan 11 10:00:00 cantata postfix/cleanup[80270]: 4052C02B56: num_local=1 num_remote=0 made_in_mx=0 untrusted=1 precedence=
Jan 11 10:00:00 cantata postfix/cleanup[80270]: 4052C02B56: fullname=, sender=frank@hifive.ca, from=, recip=sking@borderware.com,
Final action: Quarantine, Antivirus
Anti-Virus: Kaspersky virus=1
Malformed: no Attachments: off, White/Black List: no match
DCC: passed STA: metric=99, spam=yes OCF: off RBL: off
Jan 11 10:00:00 cantata postfix/smtpd[90047]: disconnect from unknown[10.1.25.1]
Jan 11 10:00:00 cantata postfix/smtpd[79169]: connect from unknown[10.1.25.1]
Jan 11 10:00:00 cantata postfix/cleanup[92025]: DDBC62D420: entry_time=1105466400.470362
Jan 11 10:00:00 cantata postfix/smtpd[79169]: DDBC62D420: helo=[127.0.0.1]
Jan 11 10:00:00 cantata postfix/smtpd[79169]: DDBC62D420: client=unknown[10.1.25.1] untrusted=1
Jan 11 10:00:00 cantata postfix/cleanup[92025]: DDBC62D420: subject=Business Opportunity
Jan 11 10:00:00 cantata postfix/cleanup[92025]: DDBC62D420: message-id=<20050111180000.DDBC62D420@cantata.borderware.com>
Jan 11 10:00:00 cantata postfix/dcc_scanner[95655]: 6D3872B1D8: DCC: dcc_resolve_host(dcc.3com.borderware.com): Unknown host
Jan 11 10:00:00 cantata newsyslog[99110]: logfile turned over

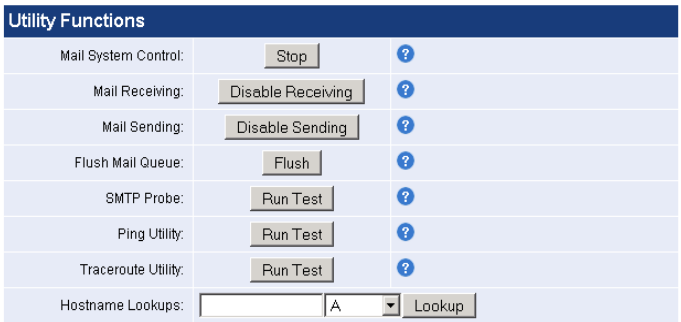
The start of a single message log entry begins with an smtpd "connect" message, and ends with the "disconnect" message. To ensure that you are looking at the entries for a specific message, check the message ID, such as *6D3872B1D8*.

A summary of the actions for this message are included in the log. In the following example, the message was quarantined because of a virus:

Final action: Quarantine, Antivirus
Anti-Virus: Kaspersky virus=1
Malformed: no Attachments: off, White/Black List: no match
DCC: passed STA: metric=99, spam=yes OCF: off RBL: off

Utility Functions

In the **System Mgmt -> Status and Utility** screen, there are utilities that can be used to help troubleshoot network connectivity and mail queue issues.



- Flush Mail Queue — Use this utility if you have a high amount of deferred mail that you would like to try and delivery. In environments with a high amount of deferred mail, this process can take a very long time. If the deferred mail queue continues to grow, there are other problems that are preventing the delivery of mail and the **Flush** button should not be clicked again.
- SMTP Probe — The SMTP (Simple Mail Transport Protocol) Probe is used to test email connectivity with a remote SMTP server. This allows you to verify that a certain SMTP server is responding to connection requests and returning a valid response. If you are having trouble delivering mail to a specific server, test your SMTP connection using this utility.
- Ping and Traceroute — Use the **Ping** and **Traceroute** utilities to ensure network connectivity with another host. From the 3Com Email Firewall, try to ping hosts both on the internal and external networks. You should also try to ping the firewall, DNS server, and external router. Try to ping the 3Com Email Firewall from these locations to ensure you have connectivity.

  Traceroute is used to see the routing steps between two hosts. If you do not have connectivity, you can use traceroute to see where exactly the packet is losing its connection.
- Hostname Lookups — Use this test to ensure that hostnames are being properly resolved by the DNS server.

Troubleshooting Content Issues

If the mail has been delivered to the 3Com Email Firewall successfully, it will undergo security processing before delivery to its final destination. Many of the security tools used by the 3Com Email Firewall, such as Anti-Spam, Content Filtering, Anti-Virus scanning, Attachment Control, and so on, will cause the message to be rejected, discarded, and quarantined without the message being delivered to the recipient's mail box.

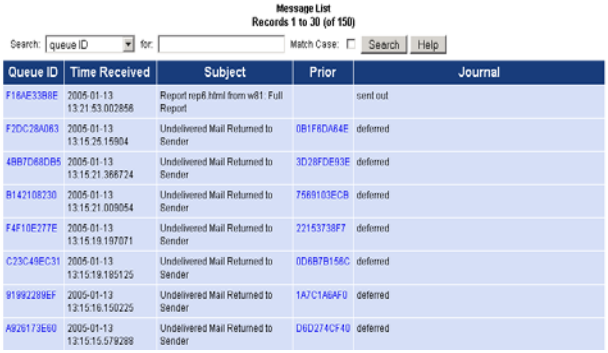
These tools can often be misconfigured allowing legitimate messages to be incorrectly rejected or quarantined. If you find that certain mail messages are being blocked when they should not be, check the following:

- Is there a Specific Access Pattern or Pattern Based Message Filter rule that applies to the message?
- Is the attachment type filtered via Attachment Control?
- Are the spam controls blocking the message?
- Is the message over the maximum size limit?

Email History

Every message that passes through the 3Com Email Firewall generates a database entry that records information about how it was processed, filtered, quarantined, and so on. To see how the message was handled by the 3Com Email Firewall, you can check the *Email History* to see the disposition of the message. Using this information, you can find out which security processing is blocking the message and then check the configuration and rules to ensure that they are set properly.

Select **Reporting -> Email History** from the menu.


Message List
Records 1 to 30 (of 150)
Search: queue ID for: Match Case: Search Help
Queue ID
Time Received
Subject
Prior
Journal
F16AE33B8E 2005-01-13 13:21:53.002868 Report rep8.html from w81: Full Report sent out
F2DC28A063 2005-01-13 13:15:25.15804 Undelivered Mail Returned to Sender 0B1F8DA64E deferred
4BB7D68DB5 2005-01-13 13:15:21.366724 Undelivered Mail Returned to Sender 3D28FDE93E deferred
B142108230 2005-01-13 13:15:21.009054 Undelivered Mail Returned to Sender 7569103ECB deferred
F4F10E277E 2005-01-13 13:15:19.197071 Undelivered Mail Returned to Sender 22153738F7 deferred
C23C49EC31 2005-01-13 13:15:19.185125 Undelivered Mail Returned to Sender 0D6B7B168C deferred
919922B9EF 2005-01-13 13:15:16.150225 Undelivered Mail Returned to Sender 1A7C1A6AF0 deferred
A926173E60 2005-01-13 13:15:15.579288 Undelivered Mail Returned to Sender D6D274CF40 deferred

Click on a specific message to see the details of its processing and final disposition.

Message Details

Message:	number 57, queue id D77125F561, size 918 bytes
Message ID:	20041221212921.D77125F561@mazurka
Prior Message:	
Subject:	Business Opportunity
From:	envelope user@example.com
Number Recipients:	local 1, remote 0
Source:	outside mazurka, message was not trusted, SSL/TLS not used
Sending Host:	fqdn mozar ip 10.1.25.1, helo [127.0.0.1]
Processing Journal:	STA spam=no, DCC passed, no virus, not malformed, sent out, STA metric 82
Times:	entered at 2004-12-21 16:29:21.467654, disposed at 2004-12-21 16:29:21.786371

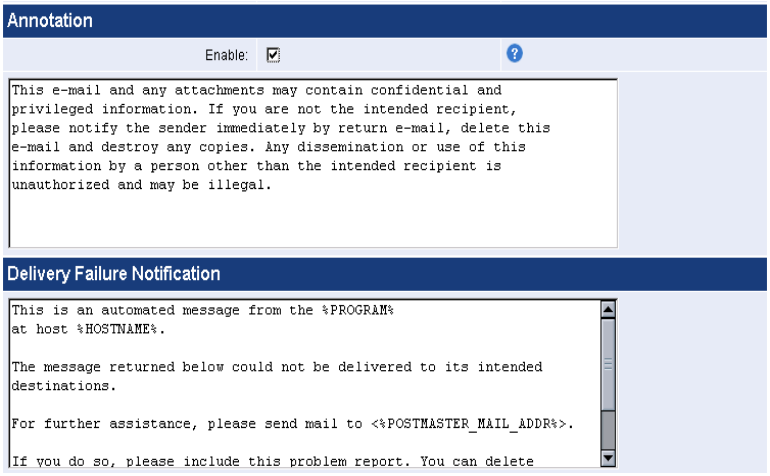
Message Disposition

Disposition	Details	Recipient, Outbound Host	Date
sent out	250 Ok: queued as 9F793A41CD	10.10.0.88 [10.10.0.88]	2004-12-21 16:29:21

A Customizing System Messages

Message variables can be used to customize the content of notification, annotation, and delivery messages. The 3Com Email Firewall will substitute your local settings for the variables at the time the message is sent.

For example, in the following *Delivery Failure Notification* message from **Mail Delivery -> Delivery Settings**, the *%HOSTNAME%* variable will be replaced with the hostname of your 3Com Email Firewall.


Annotation
Enable:
This e-mail and any attachments may contain confidential and privileged information. If you are not the intended recipient, please notify the sender immediately by return e-mail, delete this e-mail and destroy any copies. Any dissemination or use of this information by a person other than the intended recipient is unauthorized and may be illegal.
Delivery Failure Notification
This is an automated message from the %PROGRAM% at host %HOSTNAME%.
The message returned below could not be delivered to its intended destinations.
For further assistance, please send mail to <%POSTMASTER_MAIL_ADDR%>.
If you do so, please include this problem report. You can delete

The following variables can be used:

Table 5 System Message Variables

Variable	Value	Example
%PROGRAM% or %PRODUCT%	3Com Email Firewall	

Variable	Value	Example
%HOSTNAME%	Hostname entered on the Network Settings screen	mail.example.com
%POSTMASTER_MAIL_ADDR%	Email address of the admin user	admin@example.com
%DELAY_WARN_TIME%	In Delivery Settings - Time before Delay Warning	4 hours
%MAX_QUEUE_TIME%	In Delivery Settings - Maximum Time in Mail Queue	5 days
%S_YOU% or (%SENDER%)	Mail address of sender	sender@example.com
%R_YOU% or (%RECIPIENT%)	Mail address of recipient	recipient@example.com
%SPAM_FOLDER%	The name of the spam folder for the user spam quarantine	spam_quarantine
%SPAM_EXPIRY%	The number of days before quarantined spam is expired	30
%SPAM_MESSAGES%	The information for a spam message (Date,From,Subject)	05/27/04, user@example.com, File for you
%DISPN%	Disposition or Action	quarantined

B Reset to Factory Default Settings from Console

If you need to return the 3Com Email Firewall to its factory default settings, you should use the **System Mgmt -> Factory Settings** screen from the main menu.

If you have forgotten your admin password, it cannot be recovered and you will not be able to login to the 3Com Email Firewall. In this case, the system must be reset to factory default settings from the system console.

CAUTION: *After returning your system to factory default settings, do not perform a restore from a previous backup because you will overwrite the current admin password with the previous one that was forgotten. If you forget your admin password, all settings and data will be lost and you cannot perform a restore from a previous configuration.*

Use the following procedure to return the 3Com Email Firewall to factory default settings if you cannot connect using the web admin interface:

1. Shutdown the system using the power button.
2. Connect a USB keyboard and a monitor to the 3Com Email Firewall.
3. Turn on the system.
4. As the system restarts, wait for the message that appears at the top of the screen that states "Hit 'R' to reinstall" and then press "r".
5. If you were successful, the system will reinstall and then reboot. The procedure will take approximately five minutes.
6. When the 3Com Email Firewall restarts, it will be at the factory default settings. You will need to connect to the system via a web browser to the default IP address of 192.168.1.253.
7. When connected, login with the user name **admin**, and use the default password **admin**.

8 You will need to reinstall and license the system using the Setup Wizard and License Wizard. See the *Installation Guide* for details on installing the 3Com Email Firewall.

C Third Party Copyright and License Agreements

APACHE

Apache License

Version 2.0, January 2004

http://www.apache.org/licenses/

TERMS AND CONDITIONS FOR USE, REPRODUCTION, AND DISTRIBUTION

1. Definitions.

"License" shall mean the terms and conditions for use, reproduction, and distribution as defined by Sections 1 through 9 of this document.

"Licensor" shall mean the copyright owner or entity authorized by the copyright owner that is granting the License.

"Legal Entity" shall mean the union of the acting entity and all other entities that control, are controlled by, or are under common control with that entity. For the purposes of this definition, "control" means (i) the power, direct or indirect, to cause the direction or management of such entity, whether by contract or otherwise, or (ii) ownership of fifty percent (50%) or more of the outstanding shares, or (iii) beneficial ownership of such entity.

"You" (or "Your") shall mean an individual or Legal Entity exercising permissions granted by this License.

"Source" form shall mean the preferred form for making modifications, including but not limited to software source code, documentation source, and configuration files.

"Object" form shall mean any form resulting from mechanical transformation or translation of a Source form, including but not limited to compiled object code, generated documentation, and conversions to other media types.

"Work" shall mean the work of authorship, whether in Source or Object form, made available under the License, as indicated by a copyright notice that is included in or attached to the work (an example is provided in the Appendix below).

"Derivative Works" shall mean any work, whether in Source or Object form, that is based on (or derived from) the Work and for which the editorial revisions, annotations, elaborations, or other modifications represent, as a whole, an original work of authorship. For the purposes of this License, Derivative Works shall not include works that remain separable from, or merely link (or bind by name) to the interfaces of, the Work and Derivative Works thereof.

"Contribution" shall mean any work of authorship, including the original version of the Work and any modifications or additions to that Work or Derivative Works thereof, that is intentionally submitted to Licensor for inclusion in the Work by the copyright owner or by an individual or Legal Entity authorized to submit on behalf of the copyright owner. For the purposes of this definition, "submitted" means any form of electronic, verbal, or written communication sent to the Licensor or its representatives, including but not limited to communication on electronic mailing lists, source code control systems, and issue tracking systems that are managed by, or on behalf of, the Licensor for the purpose of discussing and improving the Work, but excluding communication that is conspicuously marked or otherwise designated in writing by the copyright owner as "Not a Contribution."

"Contributor" shall mean Licensor and any individual or Legal Entity on behalf of whom a Contribution has been received by Licensor and subsequently incorporated within the Work.

2. Grant of Copyright License. Subject to the terms and conditions of this License, each Contributor hereby grants to You a perpetual, worldwide, non-exclusive, no-charge, royalty-free, irrevocable copyright license to reproduce, prepare Derivative Works of, publicly display, publicly perform, sublicense, and distribute the Work and such Derivative Works in Source or Object form.

3. Grant of Patent License. Subject to the terms and conditions of this License, each Contributor hereby grants to You a perpetual, worldwide, non-exclusive, no-charge, royalty-free, irrevocable (except as stated in this section) patent license to make, have made, use, offer to sell, sell, import, and otherwise transfer the Work, where such license applies only to those patent claims licensable by such Contributor that are necessarily infringed by their Contribution(s) alone or by combination of their Contribution(s) with the Work to which such Contribution(s) was submitted. If You institute patent litigation against any entity (including a cross-claim or counterclaim in a lawsuit) alleging that the Work or a Contribution incorporated within the Work constitutes direct or contributory patent infringement, then any patent licenses granted to You under this License for that Work shall terminate as of the date such litigation is filed.

4. Redistribution. You may reproduce and distribute copies of the Work or Derivative Works thereof in any medium, with or without modifications, and in Source or Object form, provided that You meet the following conditions:

(a) You must give any other recipients of the Work or Derivative Works a copy of this License; and (b) You must cause any modified files to carry prominent notices stating that You changed the files; and (c) You must retain, in the Source form of any Derivative Works that You distribute, all copyright, patent, trademark, and attribution notices from the Source form of the Work, excluding those notices that do not pertain to any part of the Derivative Works; and (d) If the Work includes a "NOTICE" text file as part of its distribution, then any Derivative Works that You distribute must include a readable copy of the attribution notices contained within such NOTICE file, excluding those notices that do not pertain to any part of the Derivative Works, in at least one of the following places: within a NOTICE text file distributed as part of the Derivative Works; within the Source form or documentation, if provided along with the Derivative Works; or, within a display generated by the Derivative Works, if and wherever such third-party notices normally appear. The contents of the NOTICE file are for informational purposes only and do not modify the License. You may add Your own attribution notices within Derivative Works that You distribute, alongside or as an addendum to the NOTICE text from the Work, provided that such additional attribution notices cannot be construed as modifying the License.

You may add Your own copyright statement to Your modifications and may provide additional or different license terms and conditions for use, reproduction, or distribution of Your modifications, or for any such Derivative Works as a whole, provided Your use, reproduction, and distribution of the Work otherwise complies with the conditions stated in this License.

5. Submission of Contributions. Unless You explicitly state otherwise, any Contribution intentionally submitted for inclusion in the Work by You to the Licensor shall be under the terms and conditions of this License, without any additional terms or conditions.

Notwithstanding the above, nothing herein shall supersede or modify the terms of any separate license agreement you may have executed with Licensor regarding such Contributions.

6. Trademarks. This License does not grant permission to use the trade names, trademarks, service marks, or product names of the Licensor, except as required for reasonable and customary use in describing the origin of the Work and reproducing the content of the NOTICE file.

7. Disclaimer of Warranty. Unless required by applicable law or agreed to in writing, Licensor provides the Work (and each Contributor provides its Contributions) on an "AS IS" BASIS, WITHOUT WARRANTIES OR CONDITIONS OF ANY KIND, either express or implied, including, without limitation, any warranties or conditions of TITLE, NON-INFRINGEMENT, MERCHANTABILITY, or FITNESS FOR A PARTICULAR PURPOSE. You are solely responsible for determining the appropriateness of using or redistributing the Work and assume any risks associated with Your exercise of permissions under this License.

8. Limitation of Liability. In no event and under no legal theory, whether in tort (including negligence), contract, or otherwise, unless required by applicable law (such as deliberate and grossly negligent acts) or agreed to in writing, shall any Contributor be liable to You for damages, including any direct, indirect, special, incidental, or consequential damages of any character arising as a result of this License or out of the use or inability to use the Work (including but not limited to damages for loss of goodwill, work stoppage, computer failure or malfunction, or any and all other commercial damages or losses), even if such Contributor has been advised of the possibility of such damages.

9. Accepting Warranty or Additional Liability. While redistributing the Work or Derivative Works thereof, You may choose to offer, and charge a fee for, acceptance of support, warranty, indemnity, or other liability obligations and/or rights consistent with this License. However, in accepting such obligations, You may act only on Your own behalf and on Your sole responsibility, not on behalf of any other Contributor, and only if You agree to indemnify, defend, and hold each Contributor harmless for any liability incurred by, or claims asserted against, such Contributor by reason of your accepting any such warranty or additional liability.

END OF TERMS AND CONDITIONS

Curl, Libcurl

COPYRIGHT AND PERMISSION NOTICE

Copyright (c) 1996 - 2004, Daniel Stenberg, <daniel@haxx.se>.

All rights reserved.

Permission to use, copy, modify, and distribute this software for any purpose with or without fee is hereby granted, provided that the above copyright notice and this permission notice appear in all copies.

THE SOFTWARE IS PROVIDED "AS IS", WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO THE WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT OF THIRD PARTY RIGHTS. IN NO EVENT SHALL THE AUTHORS OR COPYRIGHT HOLDERS BE LIABLE FOR ANY CLAIM, DAMAGES OR OTHER LIABILITY, WHETHER IN AN ACTION OF CONTRACT, TORT OR OTHERWISE, ARISING FROM, OUT OF OR IN CONNECTION WITH THE SOFTWARE OR THE USE OR OTHER DEALINGS IN THE SOFTWARE.

Except as contained in this notice, the name of a copyright holder shall not be used in advertising or otherwise to promote the sale, use or other dealings in this Software without prior written authorization of the copyright holder.

Cyrus-SASL

CMU libsasl
Tim Martin
Rob Earhart

Copyright (c) 2000 Carnegie Mellon University. All rights reserved.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

1. Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.

2. Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.

3. The name "Carnegie Mellon University" must not be used to endorse or promote products derived from this software without prior written permission. For permission or any other legal details, please contact Office of Technology Transfer Carnegie Mellon University 5000 Forbes Avenue Pittsburgh, PA 15213-3890 (412) 268-4387, fax: (412) 268-7395 tech-transfer@andrew.cmu.edu

4. Redistributions of any form whatsoever must retain the following acknowledgment: "This product includes software developed by Computing Services at Carnegie Mellon University (http://www.cmu.edu/computing/)."

CARNEGIE MELLON UNIVERSITY DISCLAIMS ALL WARRANTIES WITH REGARD TO THIS SOFTWARE, INCLUDING ALL IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS, IN NO EVENT SHALL CARNEGIE MELLON UNIVERSITY BE LIABLE FOR ANY SPECIAL, INDIRECT OR CONSEQUENTIAL DAMAGES OR ANY DAMAGES WHATSOEVER RESULTING FROM LOSS OF USE, DATA OR PROFITS, WHETHER IN AN ACTION OF CONTRACT, NEGLIGENCE OR OTHER TORTIOUS ACTION, ARISING OUT OF OR IN CONNECTION WITH THE USE OR PERFORMANCE OF THIS SOFTWARE.

DCC

Distributed Checksum Clearinghouse

Copyright (c) 2004 by Rhyolite Software

Permission to use, copy, modify, and distribute this software for any purpose with or without fee is hereby granted, provided that the above copyright notice and this permission notice appear in all copies.

THE SOFTWARE IS PROVIDED "AS IS" AND RHYOLITE SOFTWARE DISCLAIMS ALL WARRANTIES WITH REGARD TO THIS SOFTWARE INCLUDING ALL IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS. IN NO EVENT SHALL RHYOLITE SOFTWARE BE LIABLE FOR ANY SPECIAL, DIRECT, INDIRECT, OR CONSEQUENTIAL DAMAGES OR ANY DAMAGES WHATSOEVER RESULTING FROM LOSS OF USE, DATA OR PROFITS, WHETHER IN AN ACTION OF CONTRACT, NEGLIGENCE OR OTHER TORTIOUS ACTION, ARISING OUT OF OR IN CONNECTION WITH THE USE OR PERFORMANCE OF THIS SOFTWARE.

Copyright (c) 1987, 1993, 1994

The Regents of the University of California. All rights reserved.

File

Copyright (c) Ian F. Darwin 1986, 1987, 1989, 1990, 1991, 1992, 1994, 1995. Software written by Ian F. Darwin and others; maintained 1994-1999 Christos Zoulas.

This software is not subject to any export provision of the United States Department of Commerce, and may be exported to any country or planet.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

1. Redistributions of source code must retain the above copyright notice immediately at the beginning of the file, without modification, this list of conditions, and the following disclaimer.

2. Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.

3. All advertising materials mentioning features or use of this software must display the following acknowledgement:

   This product includes software developed by Ian F. Darwin and others.

4. The name of the author may not be used to endorse or promote products derived from this software without specific prior written permission.

THIS SOFTWARE IS PROVIDED BY THE AUTHOR AND CONTRIBUTORS ``AS IS'' AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE AUTHOR OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

FreeBSD

Copyright 1994-2004 The FreeBSD Project. All rights reserved.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.

Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.

THIS SOFTWARE IS PROVIDED BY THE FREEBSD PROJECT ``AS IS'' AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE FREEBSD PROJECT OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

The views and conclusions contained in the software and documentation are those of the authors and should not be interpreted as representing official policies, either expressed or implied, of the FreeBSD Project.

FreeType

The FreeType Project LICENSE
2000-Feb-08
Copyright 1996-2000 by David Turner, Robert Wilhelm, and Werner Lemberg

Introduction
==========

The FreeType Project is distributed in several archive packages; some of them may contain, in addition to the FreeType font engine, various tools and contributions which rely on, or relate to, the FreeType Project.

This license applies to all files found in such packages, and which do not fall under their own explicit license. The license affects thus the FreeType font engine, the test programs, documentation and makefiles, at the very least.

This license was inspired by the BSD, Artistic, and IJG (Independent JPEG Group) licenses, which all encourage inclusion and use of free software in commercial and freeware products alike. As a consequence, its main points are that:

* We don't promise that this software works. However, we will be interested in any kind of bug reports. (`as is' distribution)

* You can use this software for whatever you want, in parts or full form, without having to pay us. (`royalty-free' usage)

* You may not pretend that you wrote this software. If you use it, or only parts of it, in a program, you must acknowledge somewhere in your documentation that you have used the FreeType code. (`credits')

We specifically permit and encourage the inclusion of this software, with or without modifications, in commercial products. We disclaim all warranties covering The FreeType Project and assume no liability related to The FreeType Project.

Legal Terms
==========

Definitions

Throughout this license, the terms `package', `FreeType Project', and `FreeType archive' refer to the set of files originally distributed by the authors (David Turner, Robert Wilhelm, and Werner Lemberg) as the `FreeType Project', be they named as alpha, beta or final release.

'You' refers to the licensee, or person using the project, where `using' is a generic term including compiling the project's source code as well as linking it to form a `program' or `executable'. This program is referred to as `a program using the FreeType engine'.

This license applies to all files distributed in the original FreeType Project, including all source code, binaries and documentation, unless otherwise stated in the file in its original, unmodified form as distributed in the original archive.

If you are unsure whether or not a particular file is covered by this license, you must contact us to verify this.

The FreeType Project is copyright (C) 1996-2000 by David Turner, Robert Wilhelm, and Werner Lemberg. All rights reserved except as specified below.

1. No Warranty

THE FREETYPE PROJECT IS PROVIDED `AS IS' WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESS OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE. IN NO EVENT WILL ANY OF THE AUTHORS OR COPYRIGHT HOLDERS BE LIABLE FOR ANY DAMAGES CAUSED BY THE USE OR THE INABILITY TO USE, OF THE FREETYPE PROJECT.

2. Redistribution

This license grants a worldwide, royalty-free, perpetual and irrevocable right and license to use, execute, perform, compile, display, copy, create derivative works of, distribute and sublicense the FreeType Project (in both source and object code forms) and derivative works thereof for any purpose; and to authorize others to exercise some or all of the rights granted herein, subject to the following conditions:

* Redistribution of source code must retain this license file (`LICENSE.TXT') unaltered; any additions, deletions or changes to the original files must be clearly indicated in accompanying documentation. The copyright notices of the unaltered, original files must be preserved in all copies of source files.

* Redistribution in binary form must provide a disclaimer that states that the software is based in part of the work of the FreeType Team, in the distribution documentation. We also encourage you to put an URL to the FreeType web page in your documentation, though this isn't mandatory.

These conditions apply to any software derived from or based on the FreeType Project, not just the unmodified files. If you use our work, you must acknowledge us. However, no fee need be paid to us.

3. Advertising

Neither the FreeType authors and contributors nor you shall use the name of the other for commercial, advertising, or promotional purposes without specific prior written permission.

We suggest, but do not require, that you use one or more of the following phrases to refer to this software in your documentation or advertising materials: `FreeType Project', `FreeType Engine', `FreeType library', or `FreeType Distribution'.

As you have not signed this license, you are not required to accept it. However, as the FreeType Project is copyrighted material, only this license, or another one contracted with the authors, grants you the right to use, distribute, and modify it. Therefore, by using, distributing, or modifying the FreeType Project, you indicate that you understand and accept all the terms of this license.

4. Contacts

There are two mailing lists related to FreeType:

* freetype@freetype.org

Discusses general use and applications of FreeType, as well as future and wanted additions to the library and distribution. If you are looking for support, start in this list if you haven't found anything to help you in the documentation.

* devel@freetype.org

Discusses bugs, as well as engine internals, design issues, specific licenses, porting, etc.

* http://www.freetype.org

Holds the current FreeType web page, which will allow you to download our latest development version and read online documentation.

You can also contact us individually at:

David Turner <david.turner@freetype.org>
Robert Wilhelm <robert.wilhelm@freetype.org>
Werner Lemberg <werner.lemberg@freetype.org>

GD Graphics Library

Portions copyright 1994, 1995, 1996, 1997, 1998, 1999, 2000, 2001, 2002, 2003, 2004 by Cold Spring Harbor Laboratory. Funded under Grant P41-RR02188 by the National Institutes of Health.

Portions copyright 1996, 1997, 1998, 1999, 2000, 2001, 2002, 2003, 2004 by Boutell.Com, Inc.
Portions relating to GD2 format copyright 1999, 2000, 2001, 2002, 2003, 2004 Philip Warner.
Portions relating to PNG copyright 1999, 2000, 2001, 2002, 2003, 2004 Greg Roelofs.
Portions relating to gdttf.c copyright 1999, 2000, 2001, 2002, 2003, 2004 John Ellson (ellson@graphviz.org).
Portions relating to gdft.c copyright 2001, 2002, 2003, 2004 John Ellson (ellson@graphviz.org).
Portions relating to JPEG and to color quantization copyright 2000, 2001, 2002, 2003, 2004, Doug Becker and copyright (C) 1994, 1995, 1996, 1997, 1998, 1999, 2000, 2001, 2002, 2003, 2004 Thomas G. Lane. This software is based in part on the work of the Independent JPEG Group. See the file README-JPEG.TXT for more information.

Portions relating to GIF compression copyright 1989 by Jef Poskanzer and David Rowley, with modifications for thread safety by Thomas Boutell.

Portions relating to GIF decompression copyright 1990, 1991, 1993 by David Koblas, with modifications for thread safety by Thomas Boutell.

Portions relating to WBMP copyright 2000, 2001, 2002, 2003, 2004 Maurice Szmurlo and Johan Van den Brande.

Portions relating to GIF animations copyright 2004 Jaakko Hyvätti (jaakko.hyvatti@iki.fi)

Permission has been granted to copy, distribute and modify gd in any context without fee, including a commercial application, provided that this notice is present in user-accessible supporting documentation.

This does not affect your ownership of the derived work itself, and the intent is to assure proper credit for the authors of gd, not to interfere with your productive use of gd. If you have questions, ask. "Derived works" includes all programs that utilize the library. Credit must be given in user-accessible documentation.

This software is provided "AS IS." The copyright holders disclaim all warranties, either express or implied, including but not limited to implied warranties of merchantability and fitness for a particular purpose, with respect to this code and accompanying documentation.

Although their code does not appear in the current release, the authors also wish to thank Hutchison Avenue Software Corporation for their prior contributions.

JPEG

The authors make NO WARRANTY or representation, either express or implied, with respect to this software, its quality, accuracy, merchantability, or fitness for a particular purpose. This software is provided "AS IS", and you, its user, assume the entire risk as to its quality and accuracy.

This software is copyright (C) 1991-1998, Thomas G. Lane.

All Rights Reserved except as specified below.

Permission is hereby granted to use, copy, modify, and distribute this software (or portions thereof) for any purpose, without fee, subject to these conditions:

(1) If any part of the source code for this software is distributed, then this README file must be included, with this copyright and no-warranty notice unaltered; and any additions, deletions, or changes to the original files must be clearly indicated in accompanying documentation.

(2) If only executable code is distributed, then the accompanying documentation must state that "this software is based in part on the work of the Independent JPEG Group".

(3) Permission for use of this software is granted only if the user accepts full responsibility for any undesirable consequences; the authors accept NO LIABILITY for damages of any kind.

These conditions apply to any software derived from or based on the IJG code, not just to the unmodified library. If you use our work, you ought to acknowledge us.

Permission is NOT granted for the use of any IJG author's name or company name in advertising or publicity relating to this software or products derived from it. This software may be referred to only as "the Independent JPEG Group's software".

We specifically permit and encourage the use of this software as the basis of commercial products, provided that all warranty or liability claims are assumed by the product vendor.

Libspf

The libspf Software License, Version 1.0

Copyright (c) 2004 James Couzens & Sean Comeau All rights reserved.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

1. Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.

2. Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.

THIS SOFTWARE IS PROVIDED ``AS IS'' AND ANY EXPRESSED OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE AUTHORS MAKING USE OF THIS LICENSE OR ITS CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

ModSSL

Copyright (c) 1998-2004 Ralf S. Engelschall. All rights reserved.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

1. Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.

2. Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.

3. All advertising materials mentioning features or use of this software must display the following acknowledgment: "This product includes software developed by Ralf S. Engelschall <rse@engelschall.com> for use in the mod_ssl project http://www.modssl.org/)."

4. The names "mod_ssl" must not be used to endorse or promote products derived from this software without prior written permission. For written permission, please contact rse@engelschall.com.

5. Products derived from this software may not be called "mod_ssl" nor may "mod_ssl" appear in their names without prior written permission of Ralf S. Engelschall.

6. Redistributions of any form whatsoever must retain the following acknowledgment:

"This product includes software developed by Ralf S. Engelschall <rse@engelschall.com> for use in the mod_ssl project (http://www.modssl.org/)."

THIS SOFTWARE IS PROVIDED BY RALF S. ENGELSCHALL ``AS IS'' AND ANY EXPRESSED OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL RALF S. ENGELSCHALL OR HIS CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

Mpack

(C) Copyright 1993,1994 by Carnegie Mellon University

All Rights Reserved.

Permission to use, copy, modify, distribute, and sell this software and its documentation for any purpose is hereby granted without fee, provided that the above copyright notice appear in all copies and that both that copyright notice and this permission notice appear in supporting documentation, and that the name of Carnegie Mellon University not be used in advertising or publicity pertaining to distribution of the software without specific, written prior permission. Carnegie Mellon University makes no representations about the suitability of this software for any purpose. It is provided "as is" without express or implied warranty.

CARNEGIE MELLON UNIVERSITY DISCLAIMS ALL WARRANTIES WITH REGARD TO THIS SOFTWARE, INCLUDING ALL IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS, IN NO EVENT SHALL CARNEGIE MELLON UNIVERSITY BE LIABLE FOR ANY SPECIAL, INDIRECT OR CONSEQUENTIAL DAMAGES OR ANY DAMAGES WHATSOEVER RESULTING FROM LOSS OF USE, DATA OR PROFITS, WHETHER IN AN ACTION OF CONTRACT, NEGLIGENCE OR OTHER TORTIOUS ACTION, ARISING OUT OF OR IN CONNECTION WITH THE USE OR PERFORMANCE OF THIS SOFTWARE.

Portions of this software are derived from code written by Bell Communications Research, Inc. (Bellcore) and by RSA Data Security, Inc. and bear similar copyrights and disclaimers of warranty.

NTP

Copyright (c) David L. Mills 1992-2004

Permission to use, copy, modify, and distribute this software and its documentation for any purpose and without fee is hereby granted, provided that the above copyright notice appears in all copies and that both the copyright notice and this permission notice appear in supporting documentation, and that the name University of Delaware not be used in advertising or publicity pertaining to distribution of the software without specific, written prior permission. The University of Delaware makes no representations about the suitability this software for any purpose. It is provided "as is" without express or implied warranty.

OpenLDAP

The OpenLDAP Public License

Version 2.8, 17 August 2003

Redistribution and use of this software and associated documentation ("Software"), with or without modification, are permitted provided that the following conditions are met:

1. Redistributions in source form must retain copyright statements and notices,

2. Redistributions in binary form must reproduce applicable copyright statements and notices, this list of conditions, and the following disclaimer in the documentation and/or other materials provided with the distribution, and

3. Redistributions must contain a verbatim copy of this document.

The OpenLDAP Foundation may revise this license from time to time. Each revision is distinguished by a version number. You may use this Software under terms of this license revision or under the terms of any subsequent revision of the license.

THIS SOFTWARE IS PROVIDED BY THE OPENLDAP FOUNDATION AND ITS CONTRIBUTORS ``AS IS'' AND ANY EXPRESSED OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE OPENLDAP FOUNDATION, ITS CONTRIBUTORS, OR THE AUTHOR(S) OR OWNER(S) OF THE SOFTWARE BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

The names of the authors and copyright holders must not be used in advertising or otherwise to promote the sale, use or other dealing in this Software without specific, written prior permission. Title to copyright in this Software shall at all times remain with copyright holders.

OpenLDAP is a registered trademark of the OpenLDAP Foundation.

Copyright 1999-2003 The OpenLDAP Foundation, Redwood City, California, USA. All Rights Reserved. Permission to copy and distribute verbatim copies of this document is granted.

OpenSSH

The licences which components of this software fall under are as follows. First, we will summarize and say that all components are under a BSD licence, or a licence more free than that.

OpenSSH contains no GPL code.

1) Copyright (c) 1995 Tatu Ylonen <ylo@cs.hut.fi>, Espoo, Finland All rights reserved

As far as I am concerned, the code I have written for this software can be used freely for any purpose. Any derived versions of this software must be clearly marked as such, and if the derived work is incompatible with the protocol description in the RFC file, it must be called by a name other than "ssh" or "Secure Shell".

However, I am not implying to give any licenses to any patents or copyrights held by third parties, and the software includes parts that are not under my direct control. As far as I know, all included source code is used in accordance with the relevant license agreements and can be used freely for any purpose (the GNU license being the most restrictive); see below for details.

Note that any information and cryptographic algorithms used in this software are publicly available on the Internet and at any major bookstore, scientific library, and patent office worldwide. More information can be found e.g. at "http://www.cs.hut.fi/crypto".

The legal status of this program is some combination of all these permissions and restrictions. Use only at your own responsibility. You will be responsible for any legal consequences yourself; I am not making any claims whether possessing or using this is legal or not in your country, and I am not taking any responsibility on your behalf.

NO WARRANTY

BECAUSE THE PROGRAM IS LICENSED FREE OF CHARGE, THERE IS NO WARRANTY

FOR THE PROGRAM, TO THE EXTENT PERMITTED BY APPLICABLE LAW. EXCEPT WHEN OTHERWISE STATED IN WRITING THE COPYRIGHT HOLDERS AND/OR OTHER PARTIES PROVIDE THE PROGRAM "AS IS" WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESSED OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE. THE ENTIRE RISK AS TO THE QUALITY AND PERFORMANCE OF THE PROGRAM IS WITH YOU. SHOULD THE PROGRAM PROVE DEFECTIVE, YOU ASSUME THE COST OF ALL NECESSARY SERVICING, REPAIR OR CORRECTION.

IN NO EVENT UNLESS REQUIRED BY APPLICABLE LAW OR AGREED TO IN WRITING WILL ANY COPYRIGHT HOLDER, OR ANY OTHER PARTY WHO MAY MODIFY AND/OR REDISTRIBUTE THE PROGRAM AS PERMITTED ABOVE, BE LIABLE TO YOU FOR DAMAGES, INCLUDING ANY GENERAL, SPECIAL, INCIDENTAL OR CONSEQUENTIAL DAMAGES ARISING OUT OF THE USE OR INABILITY TO USE THE PROGRAM (INCLUDING BUT NOT LIMITED TO LOSS OF DATA OR DATA BEING RENDERED INACCURATE OR LOSSES SUSTAINED BY YOU OR THIRD PARTIES OR A FAILURE OF THE PROGRAM TO OPERATE WITH ANY OTHER PROGRAMS), EVEN IF SUCH HOLDER OR OTHER PARTY HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

2) The 32-bit CRC compensation attack detector in deattack.c was contributed by CORE SDI S.A. under a BSD-style license.

Cryptographic attack detector for ssh - source code

Copyright (c) 1998 CORE SDI S.A., Buenos Aires, Argentina. All rights reserved. Redistribution and use in source and binary forms, with or without modification, are permitted provided that this copyright notice is retained.

THIS SOFTWARE IS PROVIDED ``AS IS'' AND ANY EXPRESS OR IMPLIED WARRANTIES ARE DISCLAIMED. IN NO EVENT SHALL CORE SDI S.A. BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY OR CONSEQUENTIAL DAMAGES RESULTING FROM THE USE OR MISUSE OF THIS SOFTWARE.

Ariel Futoransky <futo@core-sdi.com> <http://www.core-sdi.com>

3) ssh-keyscan was contributed by David Mazieres under a BSD-style license. Copyright 1995, 1996 by David Mazieres <dm@lcs.mit.edu>.

Modification and redistribution in source and binary forms is permitted provided that due credit is given to the author and the OpenBSD project by leaving this copyright notice intact.

4) The Rijndael implementation by Vincent Rijmen, Antoon Bosselaers and Paulo Barreto is in the public domain and distributed with the following license:

@version 3.0 (December 2000)
Optimised ANSI C code for the Rijndael cipher (now AES)
@author Vincent Rijmen <vincent.rijmen@esat.kuleuven.ac.be>
@author Antoon Bosselaers <antoon.bosselaers@esat.kuleuven.ac.be>
@author Paulo Barreto <paulo.barreto@terra.com.br>

This code is hereby placed in the public domain.

THIS SOFTWARE IS PROVIDED BY THE AUTHORS ''AS IS'' AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE AUTHORS OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

5) One component of the ssh source code is under a 3-clause BSD license, held by the University of California, since we pulled these parts from original Berkeley code.

Copyright (c) 1983, 1990, 1992, 1993, 1995 The Regents of the University of California. All rights reserved. Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

1. Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.

2. Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.

3. Neither the name of the University nor the names of its contributors may be used to endorse or promote products derived from this software without specific prior written permission.

THIS SOFTWARE IS PROVIDED BY THE REGENTS AND CONTRIBUTORS ``AS IS'' AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE REGENTS OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

6) Remaining components of the software are provided under a standard 2-term BSD licence with the following names as copyright holders:

Markus Friedl
Theo de Raadt
Niels Provos
Dug Song
Aaron Campbell
Damien Miller
Kevin Steves
Daniel Kouril
Wesley Griffin
Per Allansson
Nils Nordman
Simon Wilkinson

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

1. Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.

2. Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.

THIS SOFTWARE IS PROVIDED BY THE AUTHOR ``AS IS'' AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE AUTHOR BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

OpenSSL

Copyright (c) 1998-2003 The OpenSSL Project. All rights reserved.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

1. Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.

2. Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.

3. All advertising materials mentioning features or use of this software must display the following acknowledgment:

"This product includes software developed by the OpenSSL Project for use in the OpenSSL Toolkit. (http://www.openssl.org/)"

4. The names "OpenSSL Toolkit" and "OpenSSL Project" must not be use to endorse or promote products derived from this software without prior written permission. For written permission, please contact openssl-core@openssl.org.

5. Products derived from this software may not be called "OpenSSL" nor may "OpenSSL" appear in their names without prior written permission of the OpenSSL Project.

6. Redistributions of any form whatsoever must retain the following acknowledgment:

"This product includes software developed by the OpenSSL Project for use in the OpenSSL Toolkit (http://www.openssl.org/)"

THIS SOFTWARE IS PROVIDED BY THE OpenSSL PROJECT ``AS IS'' AND ANY EXPRESSED OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE OpenSSL PROJECT OR ITS CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE. This product includes cryptographic software written by Eric Young (eay@cryptsoft.com). This product includes software written by Tim Hudson (tjh@cryptsoft.com).

PAM

Redistribution and use in source and binary forms of Linux-PAM, with or without modification, are permitted provided that the following conditions are met:

1. Redistributions of source code must retain any existing copyright notice, and this entire permission notice in its entirety, including the disclaimer of warranties.

2. Redistributions in binary form must reproduce all prior and current copyright notices, this list of conditions, and the following disclaimer in the documentation and/or other materials provided with the distribution.

3. The name of any author may not be used to endorse or promote products derived from this software without their specific prior written permission.

ALTERNATIVELY, this product may be distributed under the terms of the GNU General Public License, in which case the provisions of the GNU GPL are required INSTEAD OF the above restrictions. (This clause is necessary due to a potential conflict between the GNU GPL and the restrictions contained in a BSD-style copyright.)

THIS SOFTWARE IS PROVIDED ``AS IS'' AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE AUTHOR(S) BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

PHP

The PHP License, version 3.0
Copyright (c) 1999 - 2002 The PHP Group. All rights reserved.

Redistribution and use in source and binary forms, with or without modification, is permitted provided that the following conditions are met:

1. Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.

2. Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.

3. The name "PHP" must not be used to endorse or promote products derived from this software without prior written permission. For written permission, please contact group@php.net.

4. Products derived from this software may not be called "PHP", nor may "PHP" appear in their name, without prior written permission from group@php.net. You may indicate that your software works in conjunction with PHP by saying "Foo for PHP" instead of calling it "PHP Foo" or "phpfoo"

5. The PHP Group may publish revised and/or new versions of the license from time to time. Each version will be given a distinguishing version number. Once covered code has been published under a particular version of the license, you may always continue to use it under the terms of that version. You may also choose to use such covered code under the terms of any subsequent version of the license published by the PHP Group. No one other than the PHP Group has the right to modify the terms applicable to covered code created under this License.

6. Redistributions of any form whatsoever must retain the following acknowledgment:
"This product includes PHP, freely available from <http://www.php.net/>".

THIS SOFTWARE IS PROVIDED BY THE PHP DEVELOPMENT TEAM ``AS IS'' AND ANY EXPRESSED OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE PHP DEVELOPMENT TEAM OR ITS CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

Info-ZIP

Copyright (c) 1990-2003 Info-ZIP. All rights reserved.

For the purposes of this copyright and license, "Info-ZIP" is defined as the following set of individuals:

Mark Adler, John Bush, Karl Davis, Harald Denker, Jean-Michel Dubois, Jean-loup Gailly, Hunter Goatley, Ian Gorman, Chris Herborth, Dirk Haase, Greg Hartwig, Robert Heath, Jonathan Hudson, Paul Kienitz, David Kirschbaum, Johnny Lee, Onno van der Linden, Igor Mandrichenko, Steve P. Miller, Sergio Monesi, Keith Owens, George Petrov, Greg Roelofs, Kai Uwe Rommel, Steve Salisbury, Dave Smith, Christian Spieler, Antoine Verheijen, Paul von Behren, Rich Wales, Mike White

This software is provided "as is," without warranty of any kind, express or implied. In no event shall Info-ZIP or its contributors be held liable for any direct, indirect, incidental, special or consequential damages arising out of the use of or inability to use this software.

Permission is granted to anyone to use this software for any purpose, including commercial applications, and to alter it and redistribute it freely, subject to the following restrictions:

1. Redistributions of source code must retain the above copyright notice, definition, disclaimer, and this list of conditions.

2. Redistributions in binary form (compiled executables) must reproduce the above copyright notice, definition, disclaimer, and this list of conditions in documentation and/or other materials provided with the distribution. The sole exception to this condition is redistribution of a standard UnZipSFX binary (including SFXWiz) as part of a self-extracting archive; that is permitted without inclusion of this license, as long as the normal SFX banner has not been removed from the binary or disabled.

3. Altered versions--including, but not limited to, ports to new operating systems, existing ports with new graphical interfaces, and dynamic, shared, or static library versions--must be plainly marked as such and must not be misrepresented as being the original source. Such altered versions also must not be misrepresented as being Info-ZIP releases--including, but not limited to, labeling of the altered versions with the names "Info-ZIP" (or any variation thereof, including, but not limited to, different capitalizations), "Pocket UnZip," "WiZ" or "MacZip" without the explicit permission of Info-ZIP. Such altered versions are further prohibited from misrepresentative use of the ip-Bugs or Info-ZIP e-mail addresses or of the Info-ZIP URL(s).

4. Info-ZIP retains the right to use the names "Info-ZIP," "Zip," "UnZip," "UnZipSFX," "WiZ," "Pocket UnZip," "Pocket Zip," and "MacZip" for its own source and binary releases.

GLOSSARY

Attachment Control A feature that allows you to block attachments based on their extension or MIME type.

BCC Blind Carbon Copy. The copy of an email is sent to a specified address without the other recipient's knowledge.

Certificate An attachment to a message that verifies its origin.

Certificate Authority (CA) A centralized organization that verifies and issues digital certificates.

DCC Distributed Checksum Clearinghouse. An anti-spam technology that uses message checksums derived from email received from all over the Internet to determine whether messages are considered bulk mail.

DNS Domain Name System. This system maps a numerical Internet Protocol (IP) address to a more meaningful and easy-to-remember name. When you need to access another device on your network, you enter the name of the device, instead of its IP address.

ESMTP Extended SMTP. A set of extensions for the SMTP (Simple Mail Transport Protocol) for better multimedia message handling.

FTP File Transfer Protocol. A protocol based on TCP/IP for reliable file transfer.

HELO The initial identifying message sent when setting up an SMTP connection between two email servers.

HTTP Hypertext Transfer Protocol. This is a set of rules for exchanging files (text, graphic images, sound, video, and other multimedia files) on the World Wide Web.

HTTPS A secure version of HTTP using SSL (Secure Sockets Layer) encryption.

IP Internet Protocol. IP is a layer 3 network protocol that is the standard for sending data through a network. IP is part of the TCP/IP set of protocols that describe the routing of packets to addressed devices.

IP address Internet Protocol address. A unique identifier for a device attached to a network using TCP/IP. The address is written as four octets separated with periods (full-stops), and is made up of a network section, an optional subnet section and a host section.

Mailer-Daemon The name of a process running on the email server that may send out status messages.

Mail Mapping Maps an external email address to a different internal email address and vice versa.

Mail Route Defines an email domain that you accept mail for, and the internal mail server to deliver the email.

Malformed Email An email message not structured according to standards. Malformed email can be used to cause denial of service attacks and buffer overruns.

MIME Multipurpose Internet Mail Extension. A standard for identifying the type of data contained in a file based on its extension.

MX Mail Exchanger. A type of DNS record indicating the address of the email server.

NIC Network Interface Card. A circuit board installed in an endstation that allows it to be connected to a network.

NTP Network Time Protocol. A protocol for time synchronization between systems on a network.

Pattern Based Message Filtering Allows you to define a pattern to search for on an email header, envelope, or body.

PBMF See Pattern Based Message Filtering.

Ping A utility used to verify connectivity over a network by sending ICMP ping packets to another host.

Protocol A set of rules for communication between devices on a network. The rules dictate format, timing, sequencing and error control.

Quarantine A protected area for storing messages that contain viruses or are considered spam. Messages can be deleted from the quarantine or released back into an email inbox.

RBL Realtime Blackhole List. A list of servers that are considered sources of known spam.

RFC Request for Comments. A series of notes on Internet technologies. RFC's can evolve to become actual Internet standards.

SMTP Simple Mail Transfer Protocol. An IETF standard protocol used for transferring mail across a network reliably and efficiently (as defined in RFC 821).

SMTP Pipelining Several SMTP commands are sent together in the same network packet.

Specific Access Pattern Defines an access pattern to match for on a specific part of an SMTP connection.

SSL Secure Sockets Layer. A protocol for encrypting and securing private data over the Internet.

STA Statistical Token Analysis. A method of identifying spam messages based on statistical analysis of email content.

Static route A routing entry ensuring connectivity to systems on other networks.

Subnet mask A subnet mask is used to divide the device part of the IP address into two further parts. The first part identifies the subnet number. The second part identifies the device on that subnet.

Syslog A syslog server collects and stores log files from many sources.

TCP/IP Transmission Control Protocol/Internet Protocol. This is the name for two of the most well-known protocols developed for the interconnection of networks. Originally a UNIX standard, TCP/IP is now supported on almost all platforms, and is the protocol of the Internet.

TCP relates to the content of the data travelling through a network — ensuring that the information sent arrives in one piece when it reaches its destination. IP relates to the address of the endstation to which data is being sent, as well as the address of the destination network.

TLS Transport Layer Security. A protocol for encrypting and providing data integrity over the Internet.

Traceroute A utility used to verify the routing path from one network host to another.

Trusted Senders List A list of users who can bypass email security controls when mailing local users.

Virtual Mapping Redirects email for a specified email address to another one without modifying the To: or From: headers of the email.

A

Activity 115
Admin Account 86
    lost password 127
Administrator Privileges 67, 87
Advanced Anti-Spam Options 69
Annotations
    Delivery Settings 24
Anti-Spam 47
    Header 70
    Server status 118
Anti-Virus 32
    Server status 118
Archive log 77
Attachment Control 34, 123
    Attachment Types 34
Authentication log 77
Auto Generate Report 73

B

Backup and Restore 107
BCC (Blind Carbon Copy) 24
Blacklisting 39, 54
BorderWare Mail Security Services 118
Bounce 25
Bulk 51

C

Certificate Authority (CA) 41, 95
Certificates 41
Check Relays 69
Configuration Information 104
Conventions
    notice icons, About This Guide 10
    text, About This Guide 10
CPU Load 80
Current Admin and Spam Quarantine Users 104

D

Daily Tasks 106
Default Anti-Spam Action 48
Degraded mode 93
Delivery Delay Warning 24
Delivery Failure 24
Delivery Settings 23
Diagnostic utilities 100
Disable Content Scan 36
Disk Usage 81

Distributed Checksum Clearinghouse (DCC) 49
DNS 89, 103
DNS Server status 118
Domain 89
Double Bounce 26

E

Email backup 106, 109
Email History 79, 123
Encryption 41, 94
  Specific Site Policy 43
Envelope-From 38
Envelope-To 38
ESMTP (Extended SMTP) 25
Examining Log Files 121

F

Factory default settings 113, 127
Flush Mail Queue 100, 122
Forgotten admin password 127
FTP backup 106, 107, 108

G

Gateway 89
Gateway status 118
Glossary 145

H

HELO 38, 40, 101
Hostname Lookups 103, 122

I

Ignore MX 24

K

KeepOpen 20
Kernel log 77

L

License Agreements 94
License key 93
Licensed Users 118
Licensing 93

Local Disk backup 107
Local users 86
Login failure 81
Lost admin password 127

M

Mail Access 37, 70
Mail Configuration 85
Mail Filtering 37, 70
Mail Mappings 26
Mail Queue Statistics 116
Mail Queues 104, 116
Mail Received Recently 116
Mail Routing 19
Mail Server Status 116
Mail Transport log 77, 121
MAILER-DAEMON 23
Malformed Email 44
Masquerade Addresses 23
Maximum message size 39
Maximum recipients per message 39
Maybe Spam 52
Message Part 55
Message Restrictions 39
Messages log 77
MIME type 36
Minimum Free Queue Space 39
MX record 20

N

Name Server 89
Network Configuration 85
Network Interfaces 90
Network Settings 89
Notifications
    Anti-Virus 33
    Attachment Control 33, 35
    Malformed Mail 45
    Objectionable Content Filter 62
NULL Character Detect 44

O

Objectionable Content Filter 61

P

PASV mode 109, 112
Pattern Based Message Filtering (PBMF) 22, 39, 54, 123

BCC Action 60
Preferences 59
priority 58
Ping 102, 122

Q

Quarantine 105
Queue ID 79
Queue Sizes 81

R

Raw Mail Body 57
RBL (Realtime Blackhole List) 69
Reboot and Shutdown 113
Relay 23
Report Configuration 72
Report Fields 74
Reporting 15, 71
Reporting History Size 82
Reset to Factory Settings 113, 127
Restore from FTP 112
Restore from Local Disk 111
RFC 1323 90
RFC 1644 90

S

Secure Web Proxy 91
Security Connection 96, 97
Security Server status 118
Self-signed certificate 95
Setup Wizard 83
SMTP AUTH 42
SMTP Authenticated Relay 40
SMTP banner 40
SMTP Notification 25
SMTP Pipelining 25
SMTP Probe 101, 122
SMTP Security 41
Software updates 96
Spam Quarantine 63, 64, 77, 104
Expiry 105
Users 67
Specific Access Patterns 21, 38, 123
SSL 41, 42
SSL certificate 94
Static Routes 92
Statistical Token Analysis (STA) 50
Maybe Spam 52
Mode 51

Tokens 57
Training 54
Status 117
Status and Utility 99
Strip Received Headers 23
Swap usage 81
Syslog 78, 89
System History 80
System Logs 77

T

TCP extensions 90
Time Server status 118
Time Zone 84
TLS 41, 42
Token 57
Traceroute 103, 122
Troubleshooting Content Issues 123
Troubleshooting Mail Delivery Problems 120
Troubleshooting Mail Queue Problems 116
Trusted Senders List 62

U

Unopenable attachments 32
Users 86

V

Variables 125
Virtual Mappings 28
Virus pattern files 33

W

Web browser compatibility 16
Web Proxy 91
Web Server Access log 77
Web Server Encrypted Accesses log 77
Web Server Encryption Engine log 77
Web Server Errors log 77
Whitelisting 39, 54

X

X-STA Headers 53

3COM CORPORATION LIMITED WARRANTY

This warranty applies to customers located in the United States, Australia, Canada (except Quebec), Ireland, New Zealand, UK and other English language countries, and countries for which a translation into the local language is not provided.

3COM INTELLIJACK HARDWARE

3Com warrants to the end user ("Customer") that this hardware product will be substantially free from material defects in workmanship and materials, under normal use and service, for the following length of time from the date of purchase from 3Com or its authorized reseller:

Limited Lifetime, for as long as the original Customer owns the product or for 5 years after product discontinuance, whichever occurs first (not transferable to a subsequent end user). FOR NON-US CUSTOMERS: Where a limited lifetime warranty is not permitted by local law, a 10 year warranty period shall be given by 3Com. The duration of this warranty shall be modified where necessary to meet any minimum warranty required by law.

3Com's sole obligation under this express warranty shall be, at 3Com's option and expense, to repair the defective product or part, deliver to Customer an equivalent product or part to replace the defective item, or if neither of the two foregoing options is reasonably available, refund to Customer the purchase price paid for the defective product. All products that are replaced will become the property of 3Com. Replacement products or parts may be new or reconditioned. 3Com warrants any replaced or repaired product or part for ninety (90) days from shipment, or the remainder of the initial warranty period, whichever is longer.

3COM INTELLIJACK SOFTWARE

3Com warrants to Customer that each software program licensed from it, except as noted below, will, if operated as directed in the user documentation, substantially achieve the functionality described in the user documentation for a period of ninety (90) days from the date of purchase from 3Com or its authorized reseller. No updates or upgrades are provided under this warranty. 3Com's sole obligation under this express warranty shall be, at 3Com's option and expense, to refund the purchase price for the software product or replace the software product with software which meets the requirements of this warranty as described above. Customer assumes responsibility for the selection of the appropriate programs and associated reference materials.

3Com makes no warranty or representation that its software products will meet Customer's requirements or work in combination with any hardware or software products provided by third parties, that the operation of the software products will be uninterrupted or error free, or that all defects in the software products will be corrected. For any third party products listed in the 3Com software product documentation or specifications as being compatible, 3Com will make reasonable efforts to provide compatibility, except where the non-compatibility is caused by a "bug" or defect in the third party's product or from use of the software product not in accordance with 3Com's published specifications or user manual.

THIS 3COM PRODUCT MAY INCLUDE OR BE BUNDLED WITH THIRD PARTY SOFTWARE. THE WARRANTY PROVISIONS OF THIS DOCUMENT DO NOT APPLY TO SUCH THIRD PART SOFTWARE. IF A SEPARATE END USER LICENSE AGREEMENT HAS BEEN PROVIDED FOR SUCH THIRD PARTY SOFTWARE, USE OF THAT SOFTWARE WILL BE GOVRNED BY THAT AGREEMENT. FOR ANY APPLICABLE WARRANTY, PLEASE REFER TO THE END USER LICENSE AGREEMENT GOVERNING THE USE OF THAT SOFTWARE.

REGULATORY INFORMATION

FCC COMPLIANCE

This device complies with part 15 of the FCC Rules. Operation is subject to the following two conditions: (1) This device may not cause harmful interference, and (2) this device must accept any interference received, including interference that may cause undesired operation.

FCC CLASS B VERIFICATION STATEMENT

NOTE: This equipment has been tested and found to comply with the limits for a Class B digital device, pursuant to Part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference in a commercial installation. This equipment generates, uses and can radiate radio frequency energy and, if not installed and used in accordance with the instructions, may cause harmful interference to radio communications. Operation of this equipment in a residential area is likely to cause harmful interference, in which case, the user will be required to correct the interference at the user's own expense.

Changes or modifications not expressly approved by 3Com could void the user's authority to operate this equipment.

INDUSTRY CANADA (IC) COMPLIANCE STATEMENT

This Class B digital apparatus complies with Canadian ICES-003.

AVIS DE CONFORMITÉ À LA RÉGLEMENTATION D'INDUSTRIE CANADA

Cet appareil numérique de la classe B est conform à la norme NMB-003 du Canada.

EUROPEAN UNION DECLARATION OF CONFORMITY

This product is in compliance with the essential requirements and other relevant provisions of Directives 73/23/EEC and 89/336/EEC.

CE